OvisLink

www.ovislink.com.tw

AirLive RS-1000

Security Bandwidth Management

User's Manual

Contents

System	1
Admin	3
Setting	7
Date/Time	16
Language	18
Permitted IP	19
Multiple NAT	23
Hack Alert	28
Route Table	31
DHCP	35
Host Table	36
Dynamic DNS	37
Logout	42

Software Update 43
Interface 44
Address
LAN 55
LAN Group 59
WAN 63
WAN Group 67
Service
Pre-defined 72
Custom 73
Group 78
Schedule 82
QoS 87
Authentication
Policy

Outgoing 98
Incoming 105

Content Filtering

URL Blocking 114
General Blocking 119

Virtual Server

Mapped IP 122
Virtual Server 126

LOG

Traffic Log 135
Event Log 138
Connection Log 141
Log Backup 144

Alarm

Traffic Alarm 148

Event Alarm 151

Accounting Report 154

Outbound 156

Inbound 162

Statistics 168

WAN Statistics 170

Policy Statistics 171

Status 173

Interface Status 174

ARP Table 176

DHCP Clients 177

Setup Examples 178

System

The Security Bandwidth Manager Administration and monitoring control is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

1. Add and change the sub Administrator's names and passwords;
2. Back up all Security Bandwidth Manager settings into local files;
3. Set up alerts for Hackers invasion.

What is System?

"System" is the managing of settings such as the privileges of packets that pass through the Security Bandwidth Manager and monitoring controls. Administrators may manage, monitor, and configure Security Bandwidth Manager settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the Security Bandwidth Manager.

Admin: has control of user access to the Security Bandwidth Manager. He/she can add/remove users and change passwords.
Setting: The Administrator may use this function to backup Security Bandwidth Manager configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Security Bandwidth Manager back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the Security Bandwidth Manager has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP (Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.
Date/Time: This function enables the Security Bandwidth Manager to be synchronized either with an Internet Server time or with the client computer's clock.
Language: Both Chinese and English are supported in the Security Bandwidth Manager.

Multiple NAT Multiple NAT allows local port to set multiple subnet works and connect with the Internet through different WAN IP Addresses.

Address：Enables the Administrator to authorize specific internal/external IP address(s for Manager.

Hack Alert When abnormal conditions occur, the Security Bandwidth Manager will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Route Table Use this function to enable the Administrator to add static routes for the networks when the dynamic route is not efficient enough.

DHCP Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Dynamic DNS The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP

Logout Administrator logs out the Security Bandwidth Manager. This function protects your system while you are away.

Software Update The administrator can update the device's software with the latest version. Administrators may visit distributor's web site to download the latest firmware. Administrators may update the device firmware to optimize its performance and keep up with the latest fixes for intruding attacks.

Admin

On the left hand menu, click on **Setup**, and then select **Admin** below it. The current list of Administrator(s) shows up.

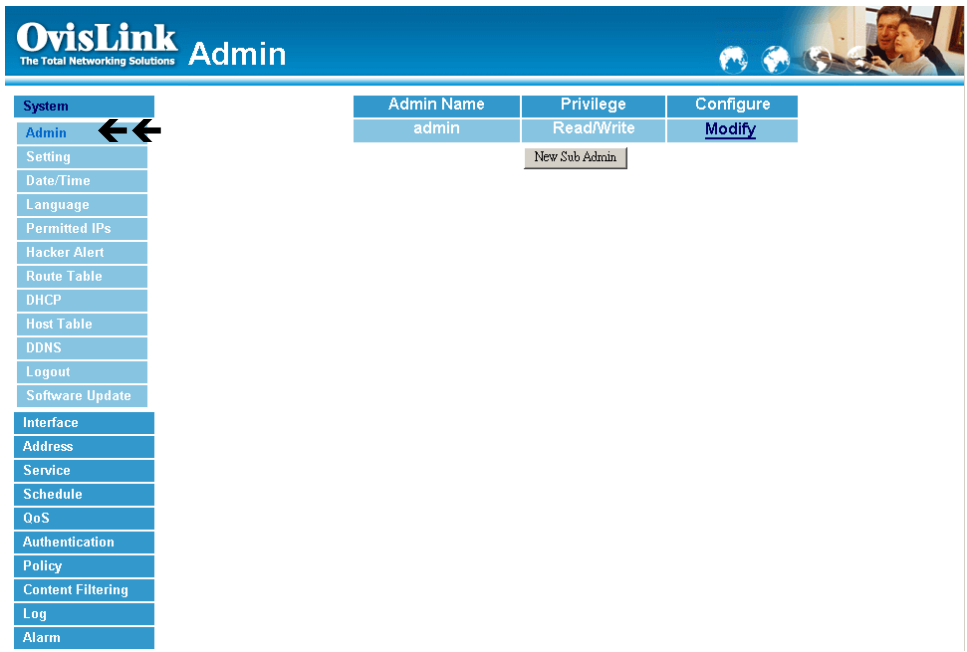


Figure1-1

Settings of the Administration table

Administrator Name: The username of Administrators for the Security Bandwidth Manager. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)

The username of the main Administrator is **Administrator** with **read / write** privilege. Sub Admins may be created by the **Admin** by clicking **New Sub Admin.** Sub Admins have **read only** privilege.

Configure: Click **Modify** to change the "Sub Administrator's" password and click **Remove** to delete a "Sub Administrator."

Changing the Main/Sub-Administrator's Password

Step 1. The **Modify Administrator Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.

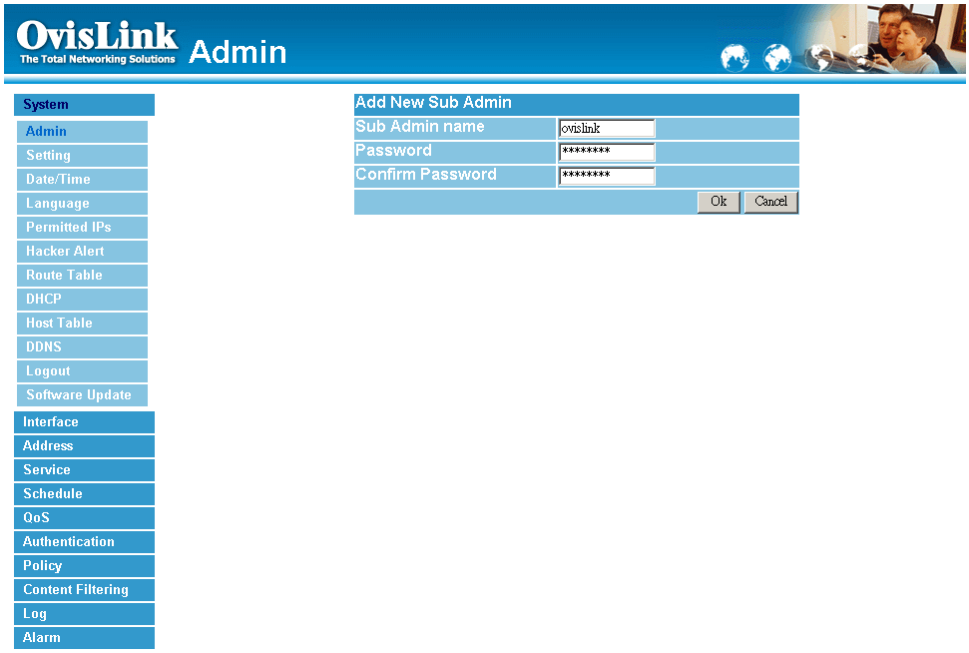


Figure1-2

Adding a new Sub Administrator

Step 1. In the **Add New Sub Administrator** window:

- **Sub Admin Name:** enter the username of new **Sub Admin.**
- **Password:** enter a password for the new **Sub Admin.**
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.

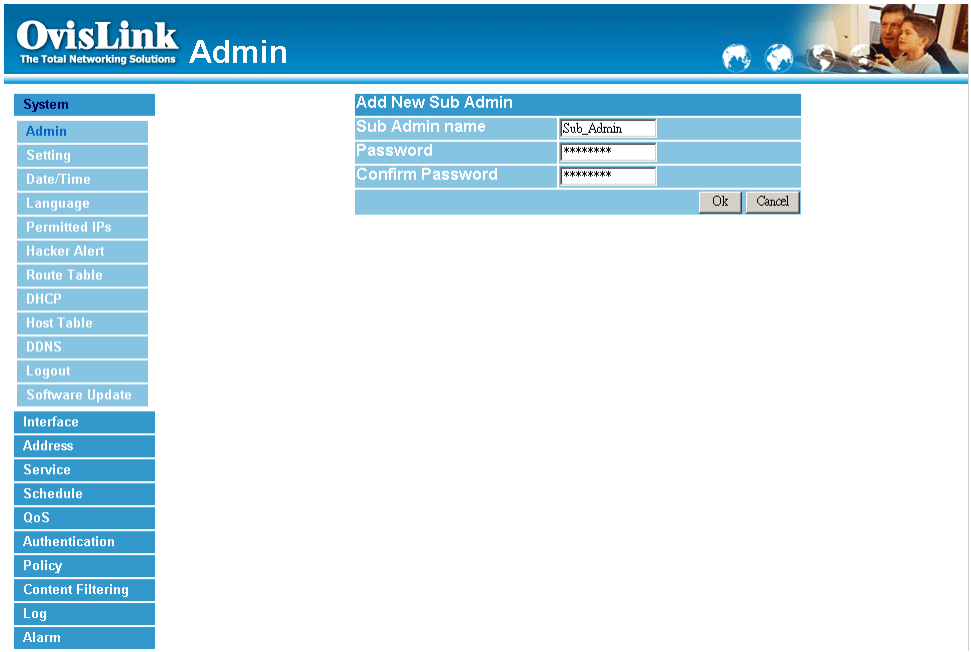


Figure 1-3

Removing a Sub Administrator

Step 1. In the Administration table, locate the Administrator name you want to edit, and click on the **Remove** option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

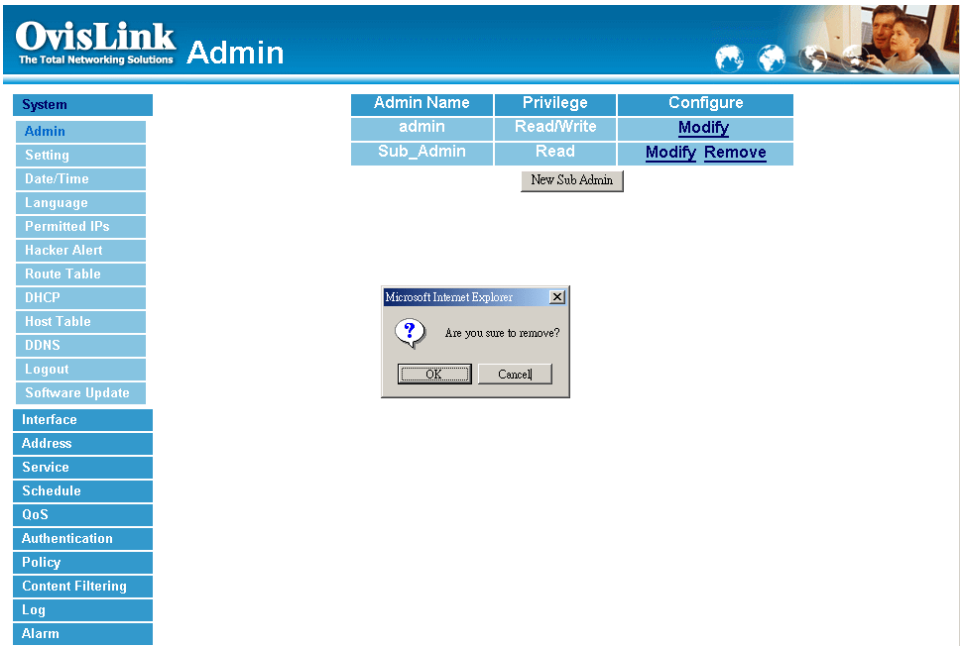


Figure1-4 Remove Sub Admin

Settings

The Administrator may use this function to backup Security Bandwidth Manager configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Security Bandwidth Manager back to default factory settings.

Entering the Settings window

Click **Setting** in the **System** menu to enter the **Settings** window. The **Bandwidth Manager Configuration** settings will be shown on the screen.

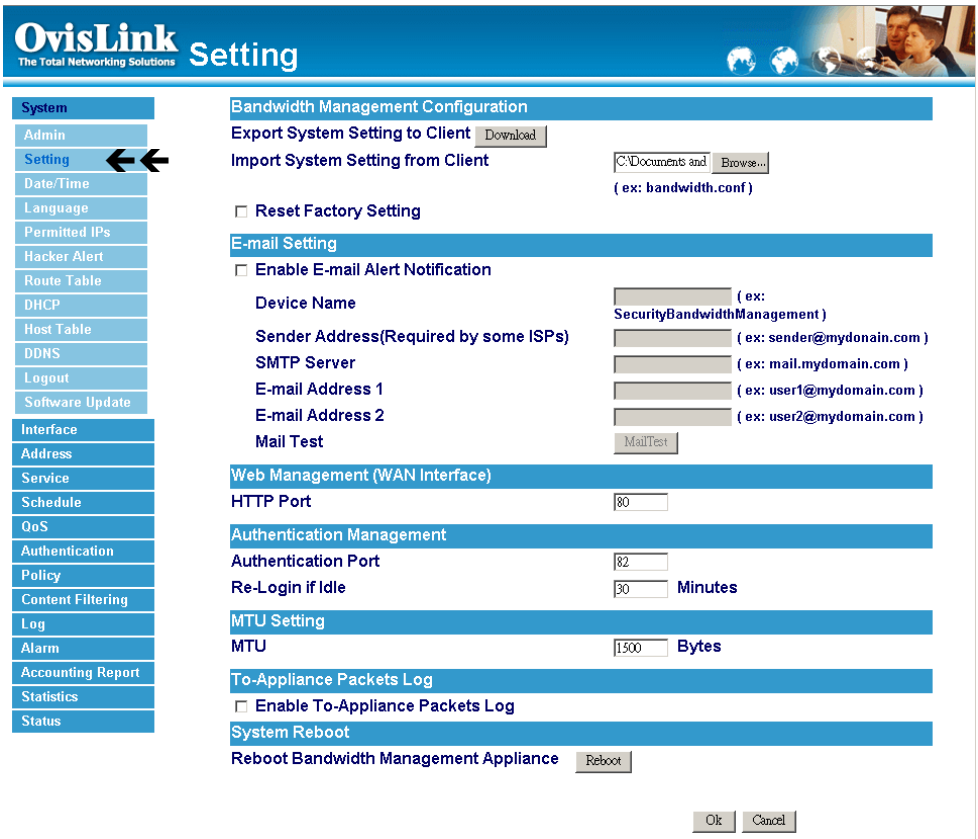


Figure1-5 Setting

Exporting Security Bandwidth Manager settings

Step 1. Under **Bandwidth Manager Configuration**, click on the **Download** button next to **Export System Settings to Client**.

Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.

Figure1-6 Select the location where the exported files to be saved

Importing Security Bandwidth Manager settings

Under **Bandwidth Manager Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file which contains the saved Security Bandwidth Manager Settings, then click **OK**.

Click **OK** to import the file into the **Security Bandwidth Manager** or click **Cancel** to cancel importing.

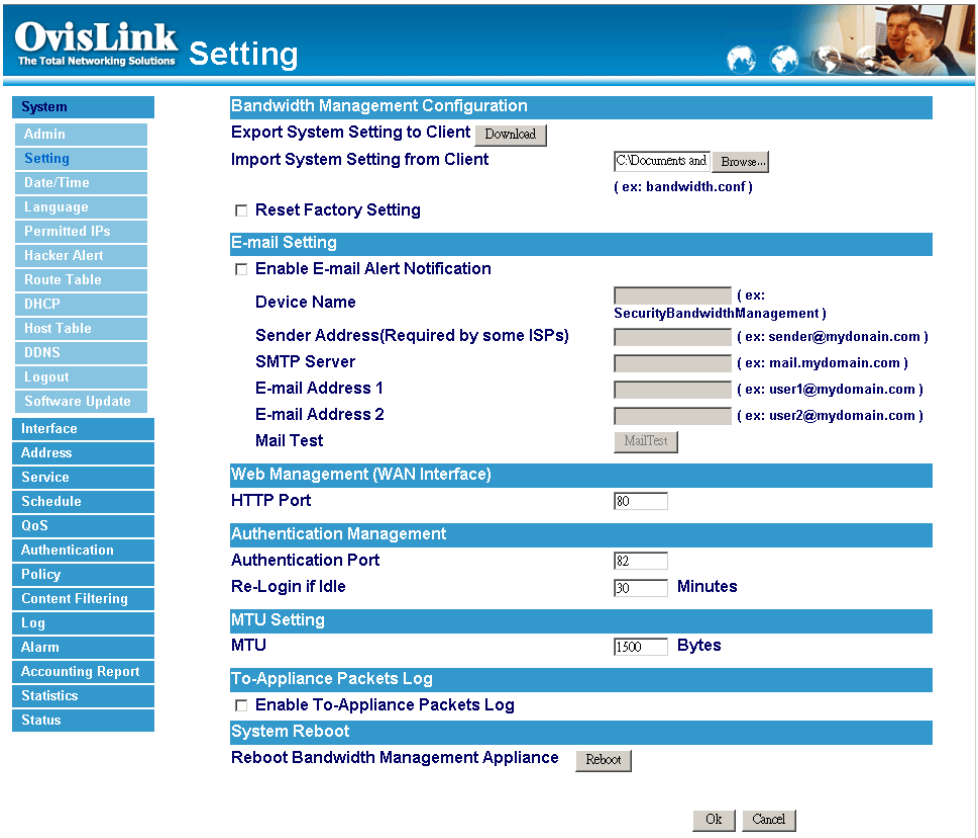


Figure1-7 Location and filename for saving imported file

Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Bandwidth Manager Configuration**.

Click **OK** at the bottom-right of the screen to restore the factory settings.

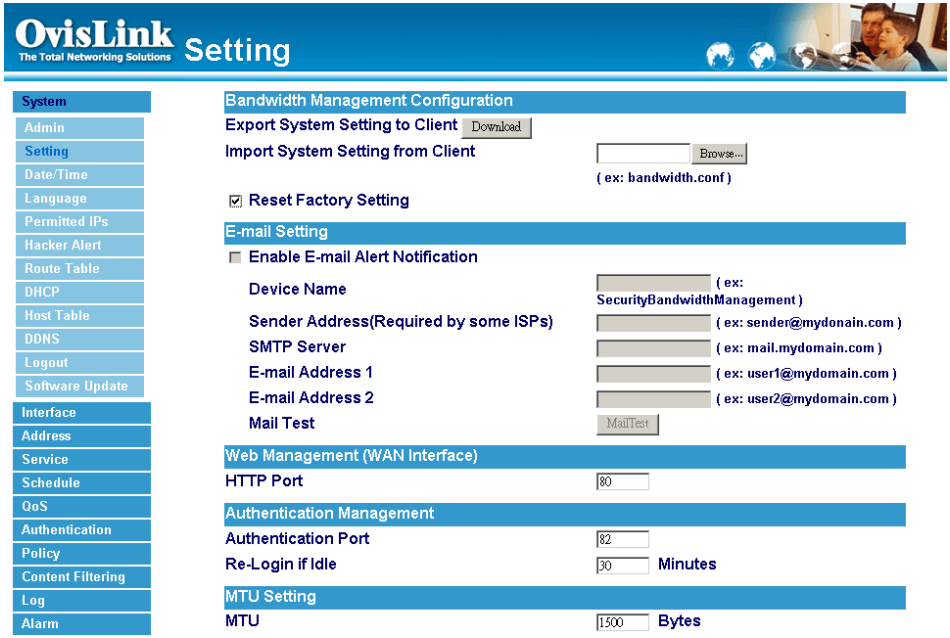


Figure1-8 Select Reset Factory Settings

Enabling E-mail Alert Notification

Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Security Bandwidth Manager to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Click **OK** on the bottom-right of the screen to enable E-mail alert notification.

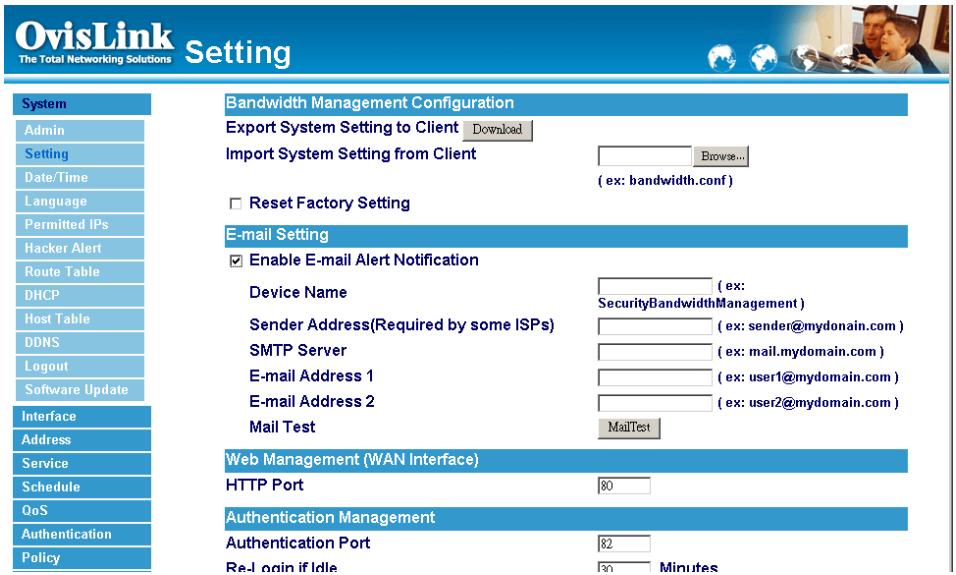


Figure1-9 Enable E-mail Alert Notification

Web Manager (WAN Interface) (Remote UI Manager)

The administrator can change the port number used by HTTP port anytime. (Remote UI Manager)

Step 1. Set Web Manager (WAN Interface). The administrator can change the port number used by HTTP port anytime.

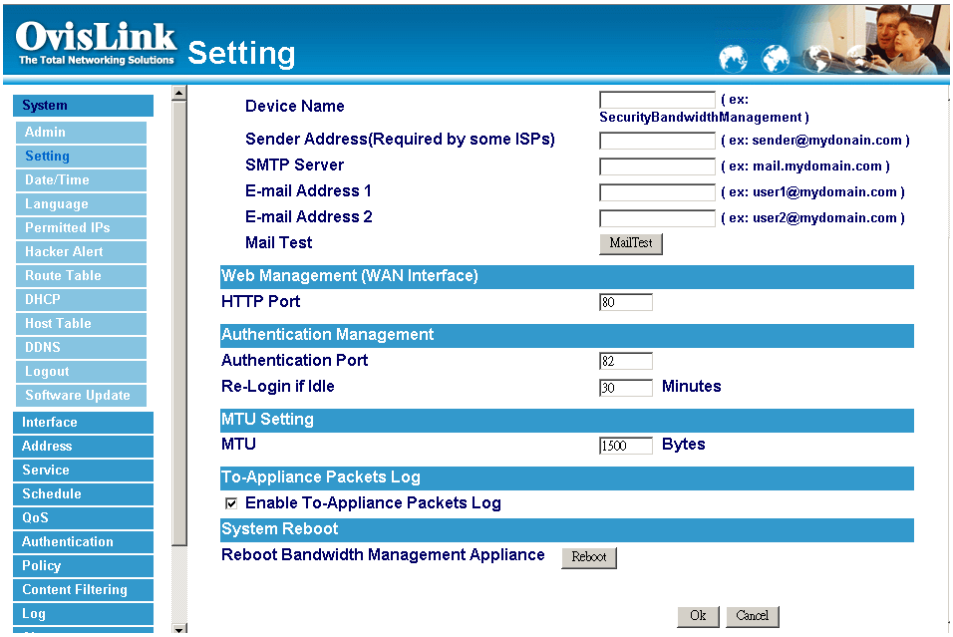


Figure1-10 Web Manager

MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. MTU Setting. Modify the networking packet length.

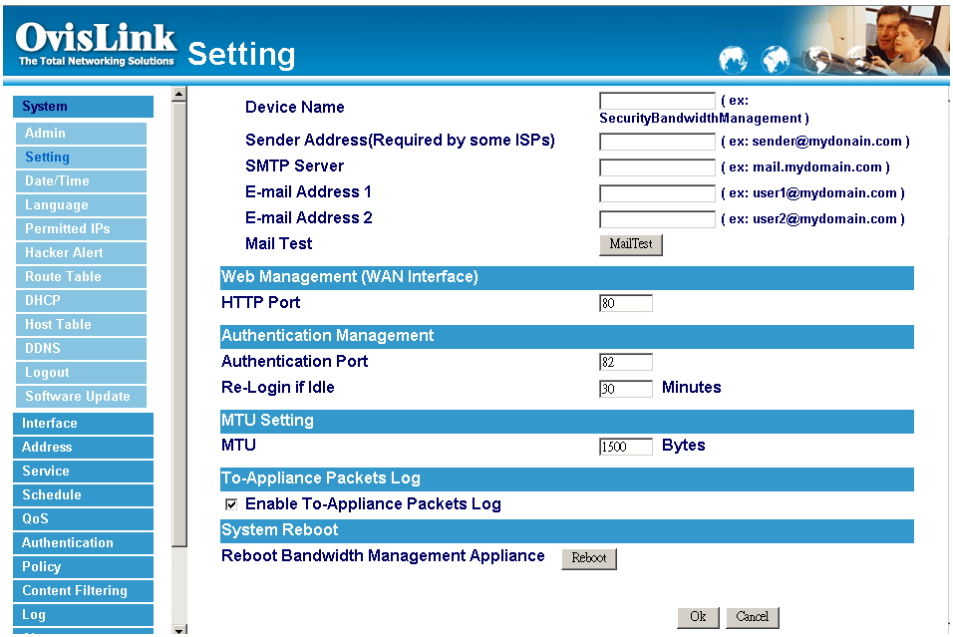


Figure1-11 MTU

To-Bandwidth Manager Packets Log

Once this function is enabled, every packet passing through the Firewall will be recorded for the administrator to trace.

Step 1. Select this option to the device's **To-Bandwidth Manager Packets Log.** Once this function is enabled, every packet to this appliance will be recorded for system manager to trace.

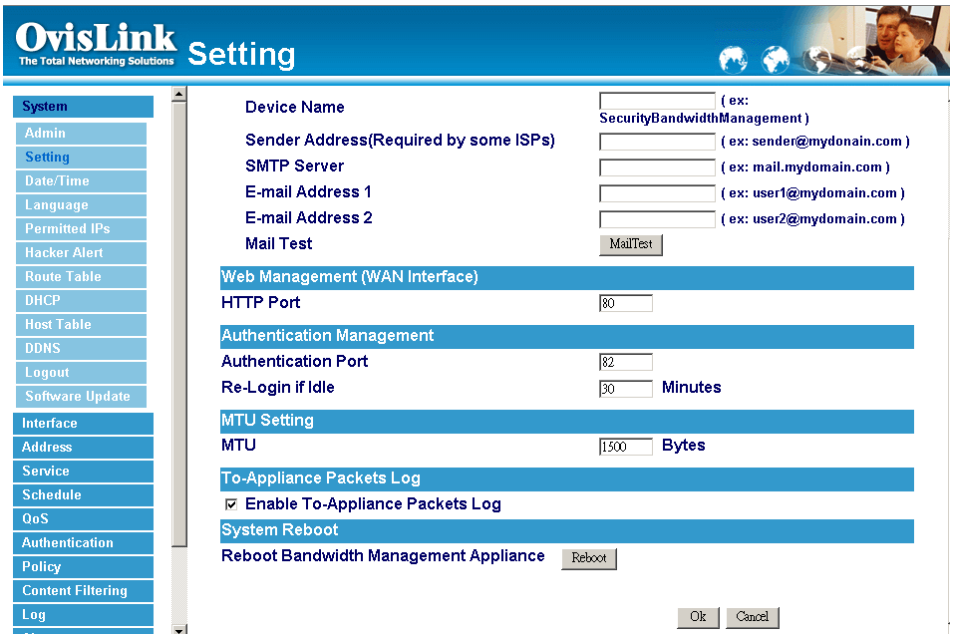


Figure1-12 Enable To Bandwidth Manager Packets Log

Security Bandwidth Manager Reboot

Once this function is enabled, the Security Bandwidth Manager will be rebooted.

Reboot Security Bandwidth Manager: Click **Reboot.**

A confirmation pop-up box will appear. Follow the confirmation pop-up box, click **OK** to restart Security Bandwidth Manager or click **Cancel** to discard changes

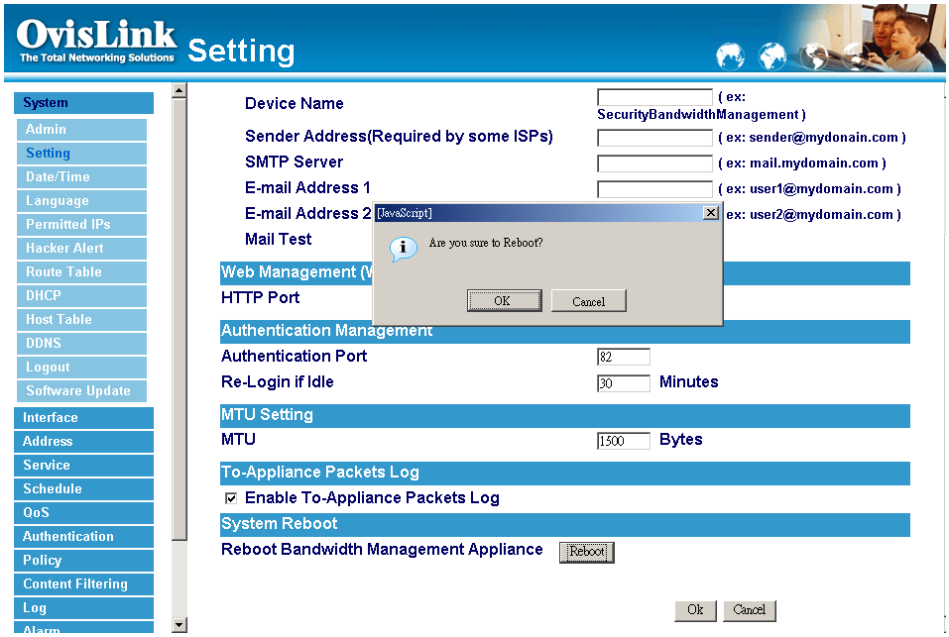


Figure1-13 Reboot Security Bandwidth Manager

Date/Time

Synchronizing the Bandwidth Manager with the System Clock

Admins can configure the Security Bandwidth Manager.s date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer.s clock.

Follow these steps to sync to an Internet Time Server

Step 1. Enable synchronization by checking the box.

Step 2. Click the down arrow to select the offset time from GMT.

Step 3. Enter the Server IP Address or Server name with which you want to synchronize.

Step 4. **Update system clock every 5 minutes** You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer's clock.

Step 1. Click on the **Sync** button.

Click **OK** to apply the setting or click **Cancel** to discard changes.

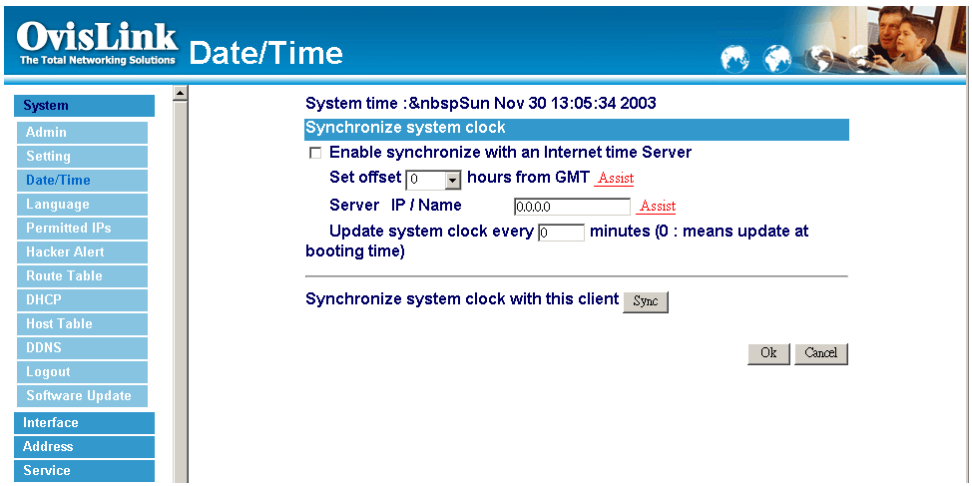


Figure1-14 System Time

Language

Admins can configure the Security Bandwidth Manager Select the Language version

Step 1. Select the Language version (**English Version/Traditional Chinese Version** or **Simplified Chinese Version**).

Step 2. Click 【**OK**】to set the Language version or click **Cancel** to discard changes.

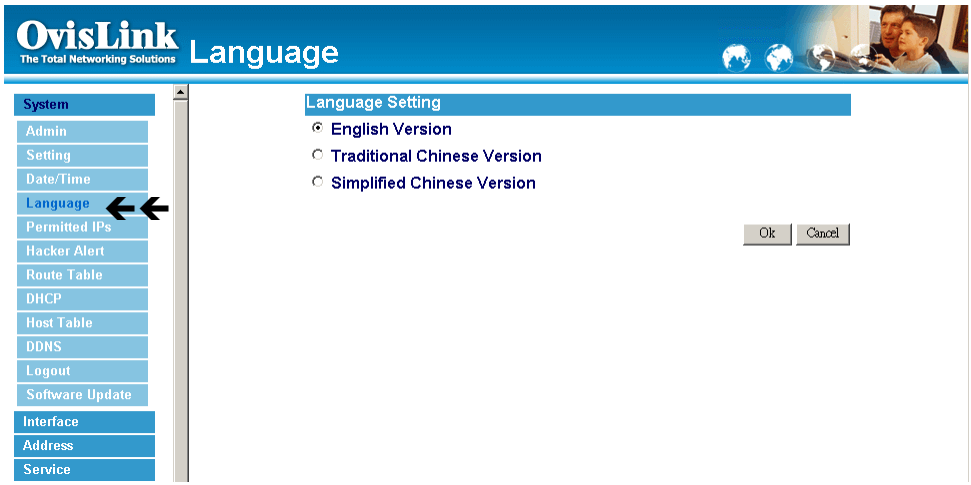


Figure1-15 Language Setting

Permitted IPs

Only the authorized IP address is permitted to manage the Security Bandwidth Manager.

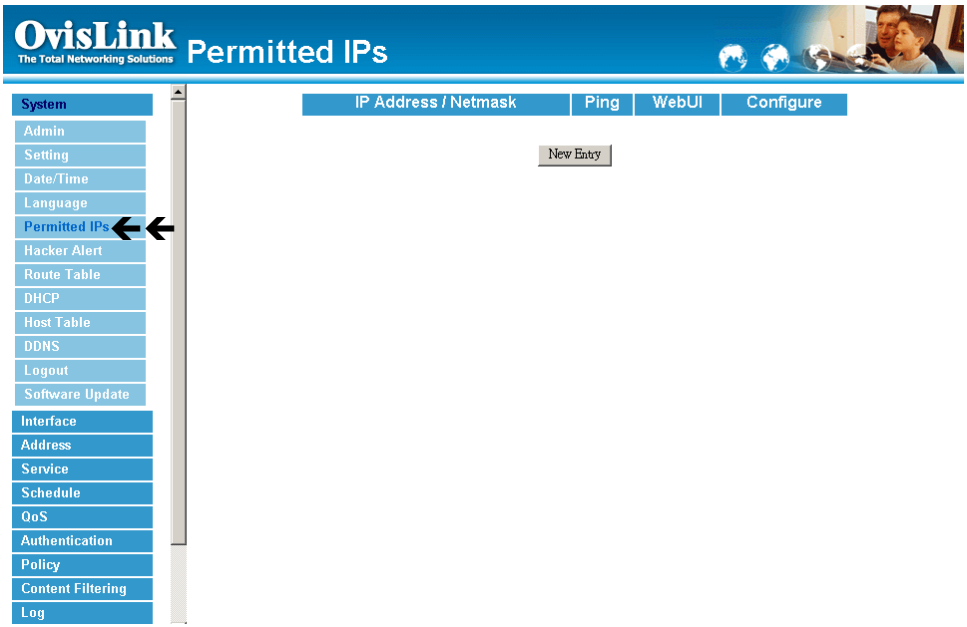


Figure1-16 Permitted IP Address

Add Permitted IP Address

Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **IP address**：Enter the LAN IP address or WAN IP address.
- **Netmask**：Enter the netmask of LAN/WAN.
- **Ping**：Select this to allow the external network to ping the IP Address of the Firewall.
- **WebUI**：Check this item, Web User can use HTTP to connect to the Setting window of Security BandWidth Manager.

Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.

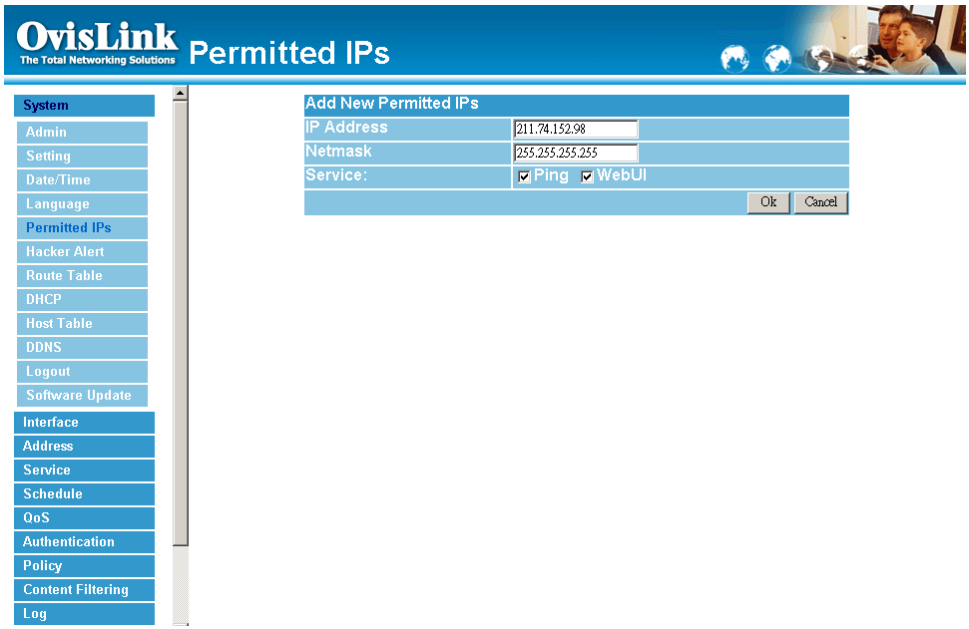


Figure1-17 Add New Permitted IPs

Modify Permitted IP Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IP**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.

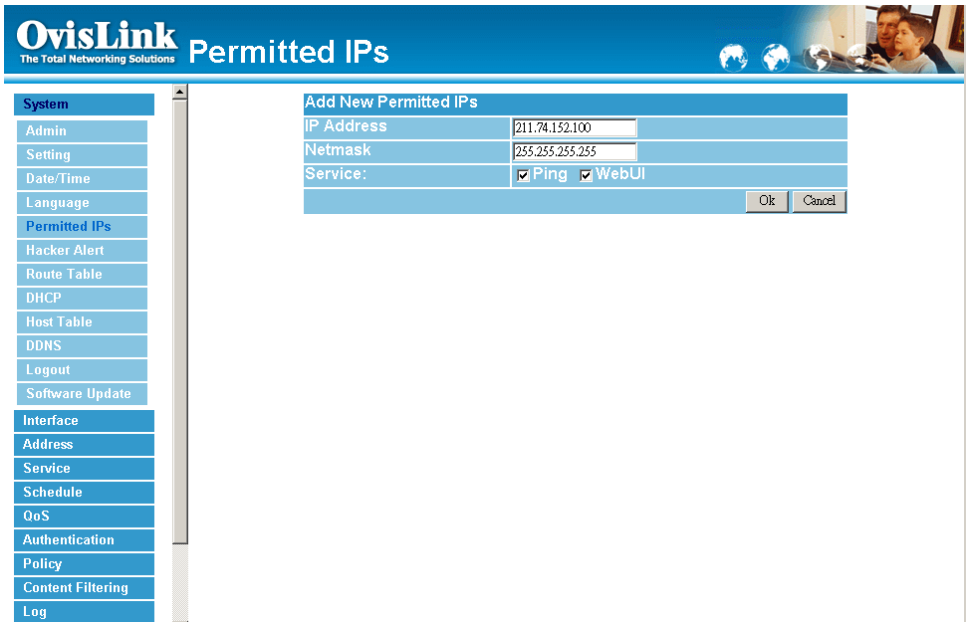


Figure1-18 Modify Permitted IPs

Remove Permitted IP addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In **Remove Permitted IP**, enter new IP address.

Step 3. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.

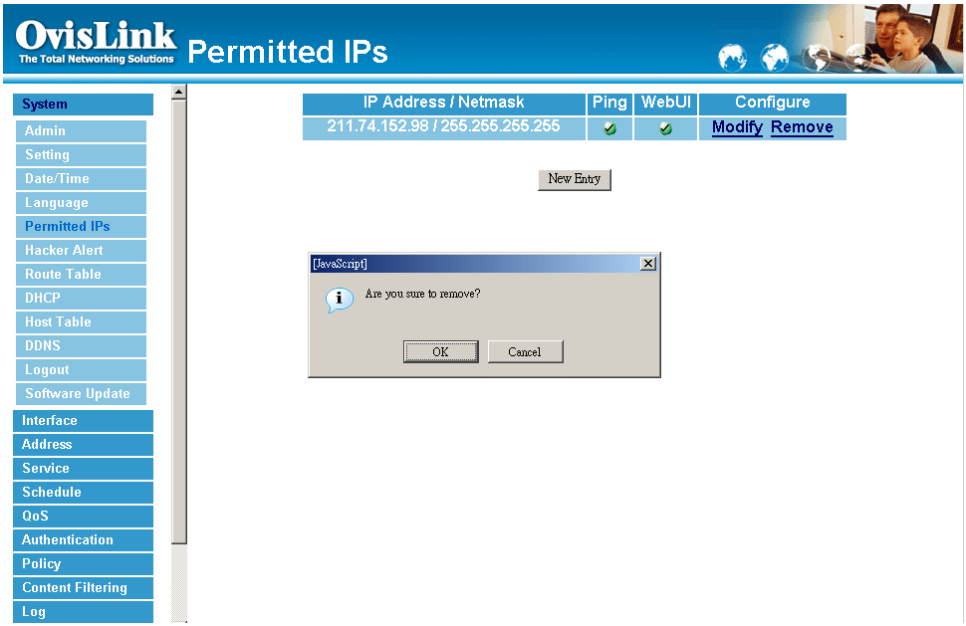


Figure1-19 Remove Permitted IPs

Multiple NAT

Multiple NAT allows local port to set multiple subnetworks and connect with the Internet through different WAN IP Addresses.

For instance：The lease line of a company applies several real IP Addresses 168.85.88.0/24，and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnetworks for the purpose of convenient Manager. The settings are as the following：

1.R&D department subnetwork：192.168.1.11/24(Internal) ←→ 168.85.88.253(WAN)

2. Service department subnetwork：192.168.2.11/24(Internal) ←→ 168.85.88.252(WAN)

3.Sales department subnetwork： 192.168.3.11/24(Internal) ←→ 168.85.88.251(WAN)

4.Procurement department subnetwork 192.168.4.11/24(Internal) ←→ 168.85.88.250(WAN)

5.Accounting department subnetwork 192.168.5.11/24(Internal) ←→ 168.85.88.249(WAN)

The first department(R&D department) was set while setting interface IP, the other four ones have to be added in Multiple NAT，after completing the settings, each department use the different WAN IP Address to connect to the Internet. The settings of each department are as the following

Service IP Address：192.168.2.1

Subnet Mask：255.255.255.0

Default Gateway：192.168.2.11

The other departments are also set by groups, this is the function of Multiple NAT.

Multiple NAT settings

Step 1. Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.

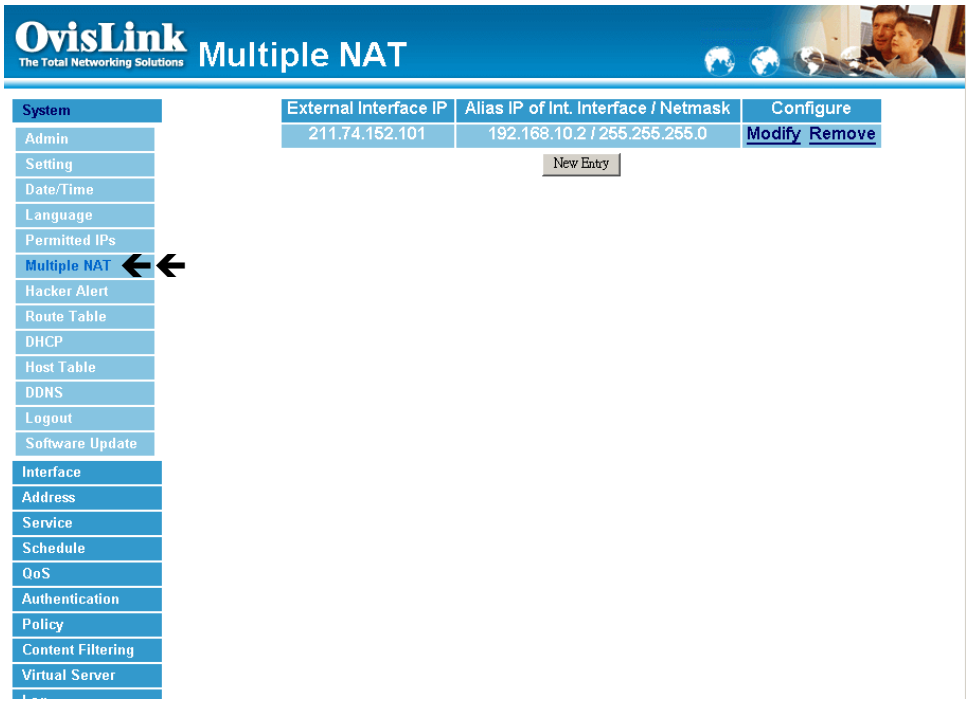


Figure1-20 Multiple NAT

Global port interface IP Address: Global port IP Address.

Local port interface IP Address: Local port IP Address and subnet Mask.

Modify: Modify the settings of Multiple NAT. Click **Modify** to modify the parameters of Multiple NAT or click **Delete** to delete settings.

Add Multiple NAT

Step 1. Click the **Add** button below to add Multiple NAT.

Step 2. Enter the IP Address in the website name column of the new window.

- **Global port interface IP Address**： Select Global port IP Address.
- **Local port interface IP Address**： Enter Local port IP Address.
- **Subnet Mask**：Enter Local port subnet Mask.

Step 3. Click **OK** to add Multiple NAT or click **Cancel** to discard changes.

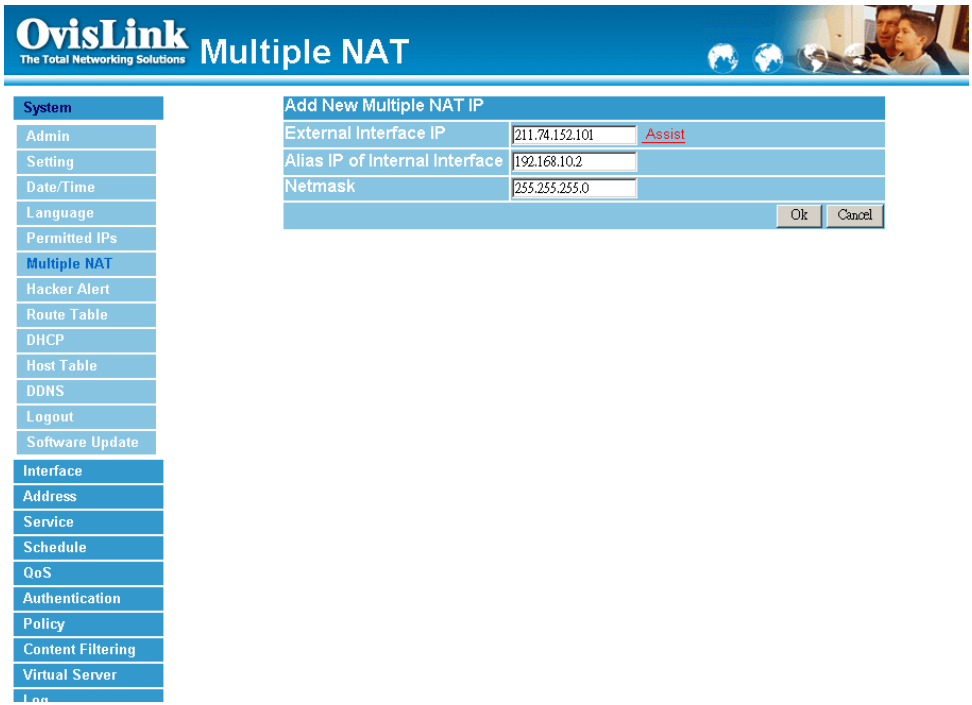


Figure1-21 Add Multiple NAT

Modify Multiple NAT

Step 1. Find the IP Address you want to modify and click **Modify**

Step 2. Enter the new IP Address in **Modify Multiple NAT** window.

Step 3. Click the **OK** button below to change the setting or click **Cancel** to discard changes.

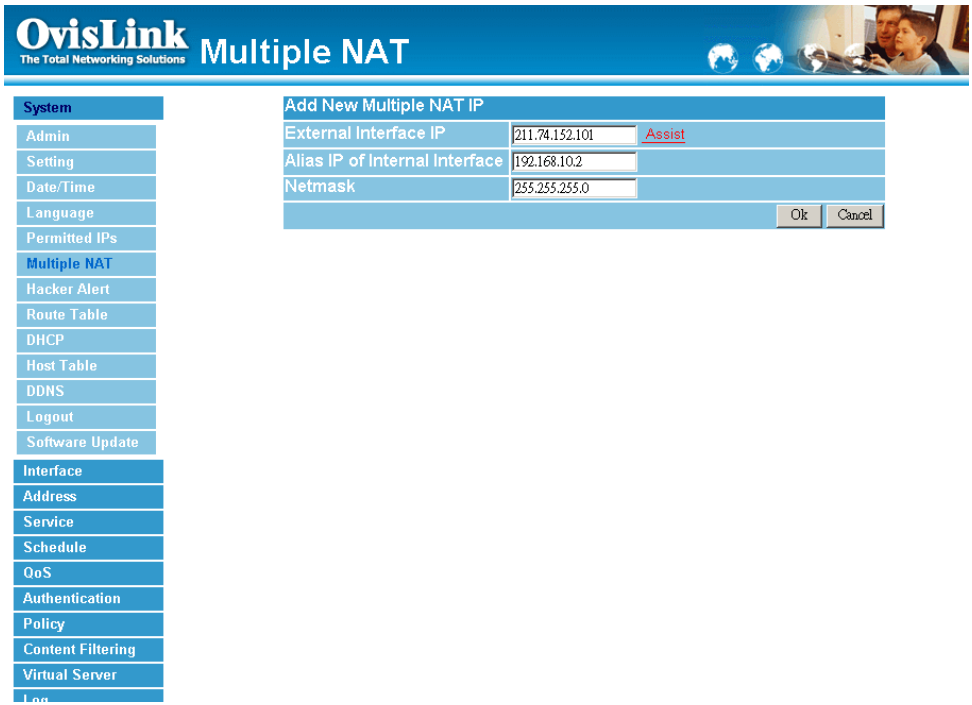


Figure1-22 Modify Multiple NAT

Delete Multiple NAT

Step 1. Find the IP Address you want to delete and click **Delete**.

Step 2. A confirmation pop-up box will appear, click **OK** to delete the setting or click **Cancel** to discard changes.

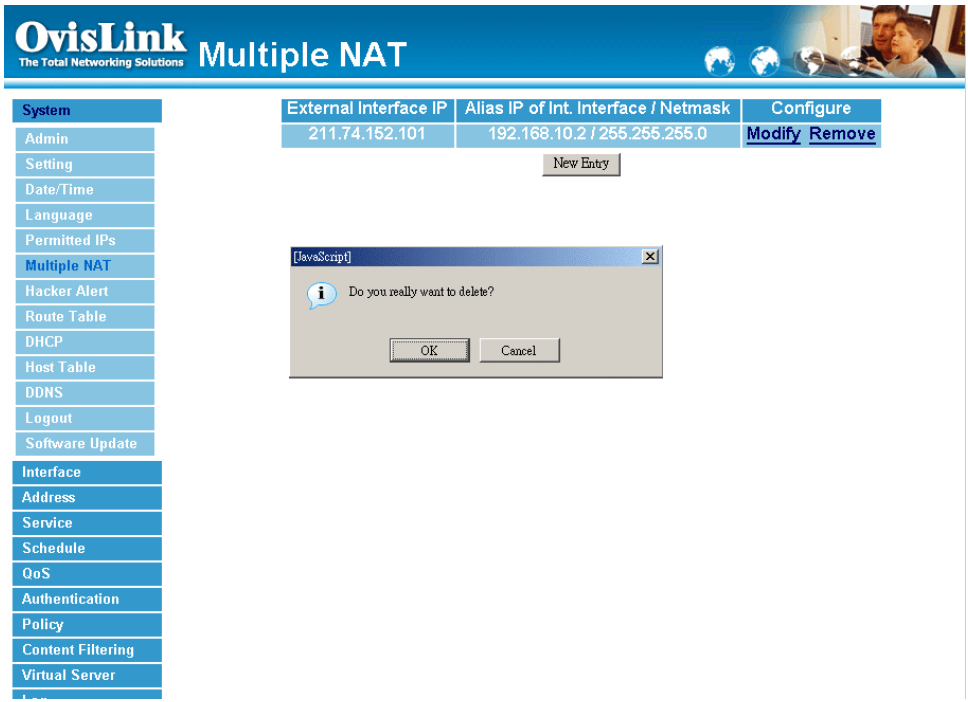


Figure1-23 Remove Multiple NAT

Hacker Alarm

The Administrator can enable the device's auto detect functions in this section. When abnormal conditions occur, the Security Bandwidth Manager will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

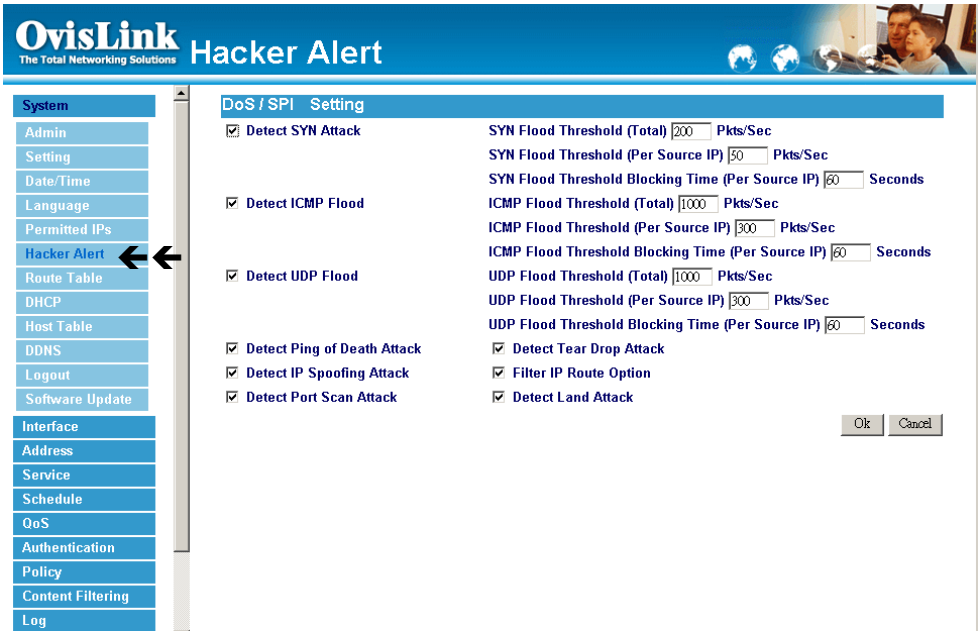


Figure1-24 Hacker Alert

Auto Detect functions

- **Detect SYN Attack**: Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will prevent valid users from connecting to the servers. After enabling this function, the System Administrator can enter the number of SYN packets per second that is allowed to enter the network/ Security Bandwidth Manager. Once the SYN packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default SYN flood threshold is set to 200 Pkts/Sec .

- **Detect ICMP Flood**: Select this option to detect ICMP flood attacks. When hackers continuously send PING packets to all the machines of the LAN networks or to the Security Bandwidth Manager, your network is experiencing an ICMP flood attack. This can cause traffic congestion on the network and slows the network down. After enabling this function, the System Administrator can enter the number of ICMP packets per second that is allowed to enter the network/ Security Bandwidth Manager. Once the ICMP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default ICMP flood threshold is set to 1000 Pkts/Sec.

- **Detect UDP Flood**: Select this option to detect UDP flood attacks. A UDP flood attack is similar to an ICMP flood attack. After enabling this function, the System Administrator can enter the number of UDP packets per second that is allow to enter the network/Bandwidth Manager. Once the UDP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default UDP flood threshold is set to 1000 Pkts/Sec .

- **Detect Ping of Death Attack**: Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.

- **Detect Tear Drop Attack**: Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.

- **Detect IP Spoofing Attack**: Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the Security Bandwidth Manager System and invade the network.

- **Filter IP Source Route Option**: Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade LAN networks and send LAN networks' data back to them.
- **Detect Port Scan Attack**: Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.
- **Detect Land Attack**: Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when SYN on the TCP header is marked.
  Enable this function to detect such abnormal packets.

After enabling the needed detect functions, click OK to activate the changes.

Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen

Step 1. Click **System** on the left side menu bar, then click **Route Table** below it. The Route Table window appears, in which current route settings are shown.

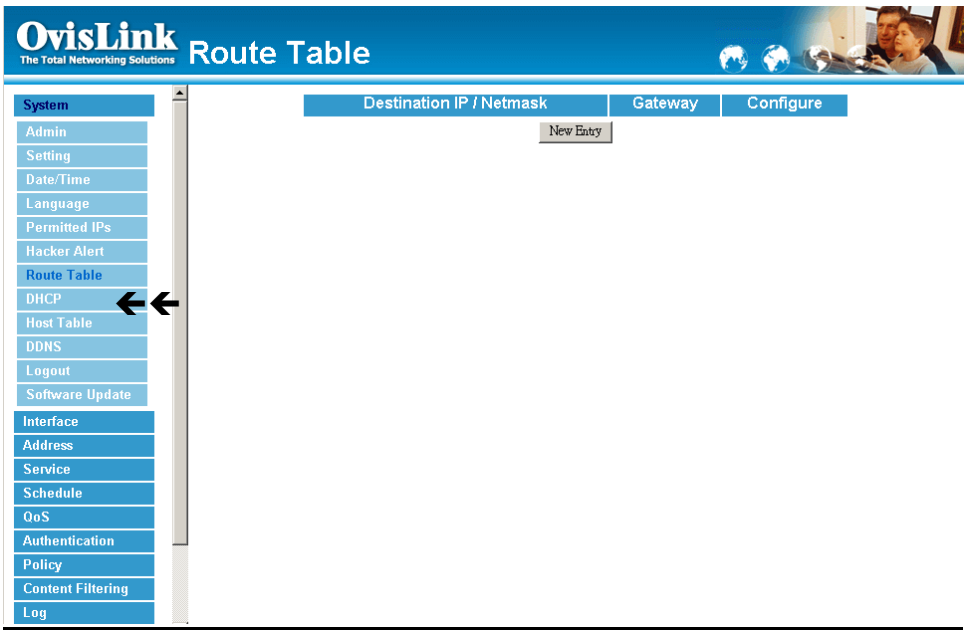


Figure1-25 Route Table

Route Table functions

- **Interface:** Destination network , LAN or WAN 1 networks.
- **Destination IP:** IP address of destination network.
- **NetMask:** Netmask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

Adding a new Static Route

Step 1. In the Route Table window, click the **New Entry** button.

Step 2. In the Add New Static Route window, enter new static route information.

Step 3. In the Interface field's pull-down menu, choose the network to connect (LAN, WAN).

Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.

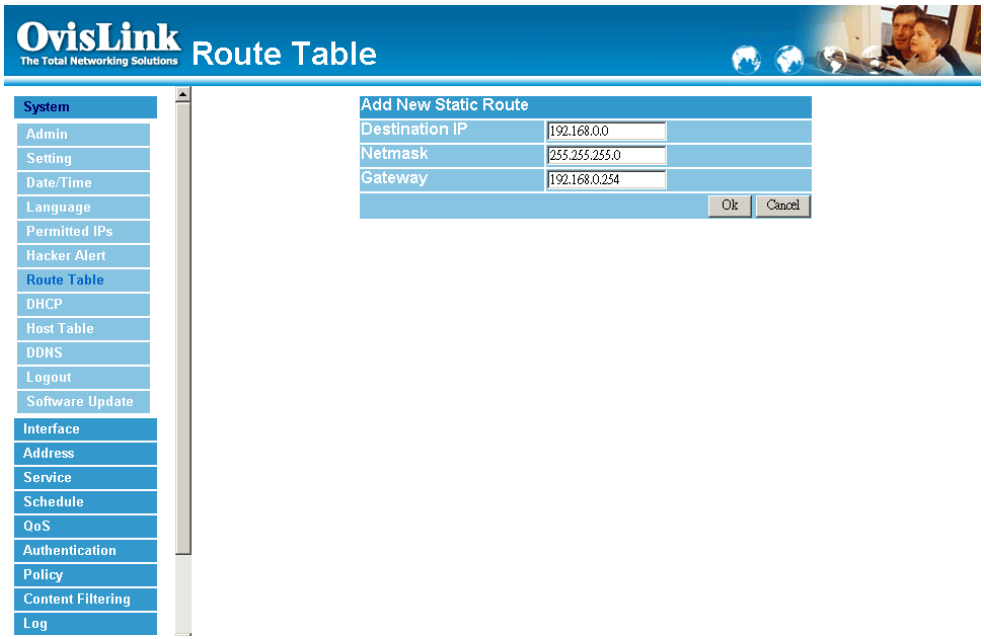


Figure1-26 Add New Static Route

Modifying a Static Route:

Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the Configure field.

Step 2. In the **Modify Static Route** window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

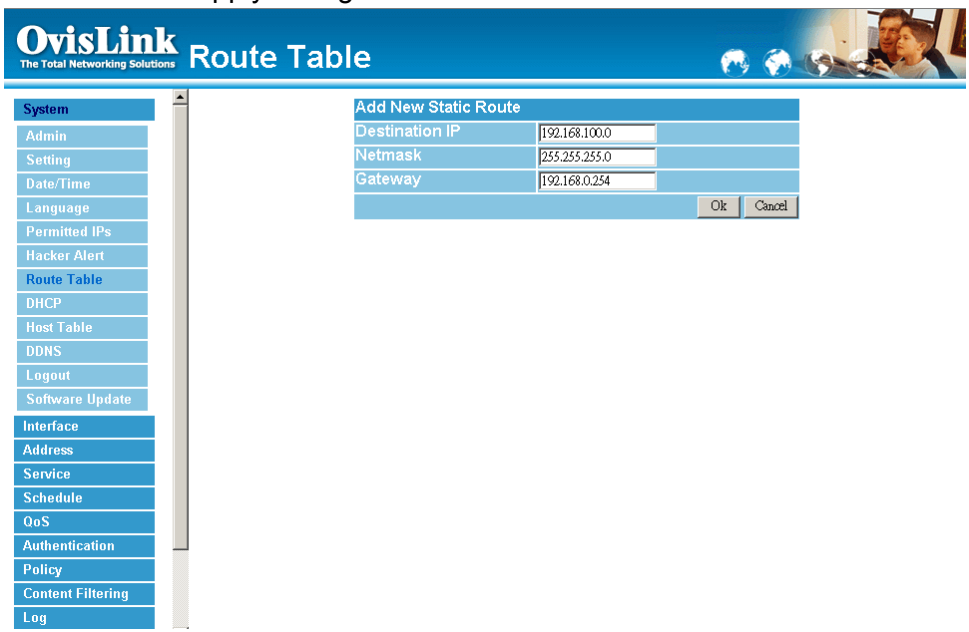


Figure1-27 Modify Static Route

Removing a Static Route

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.

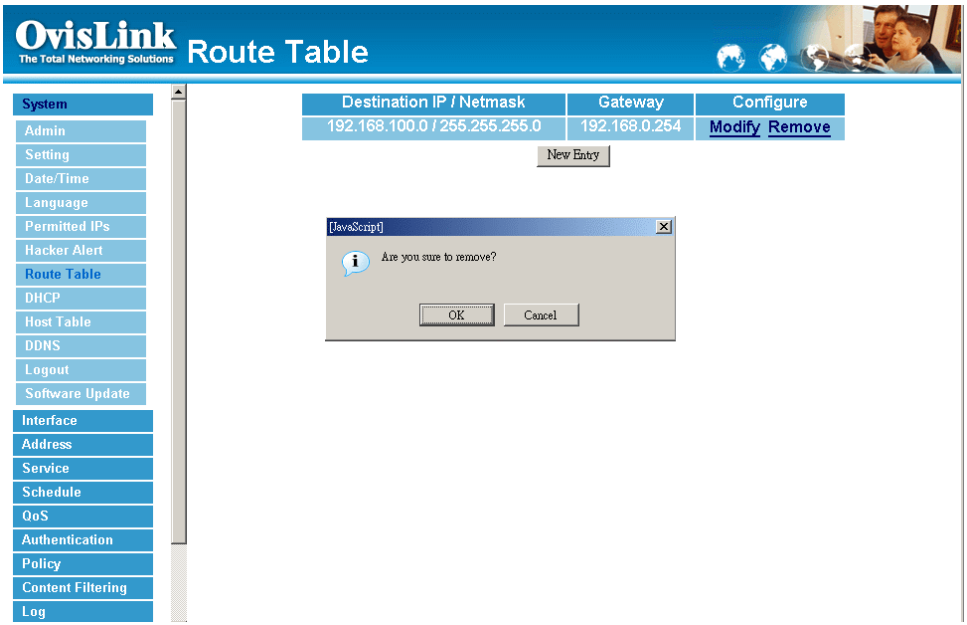


Figure1-28 Remove a Static Route

DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Entering the DHCP window

Click **System** on the left hand side menu bar, then click **DHCP** below it. The DHCP window appears in which current DHCP settings are shown on the screen.

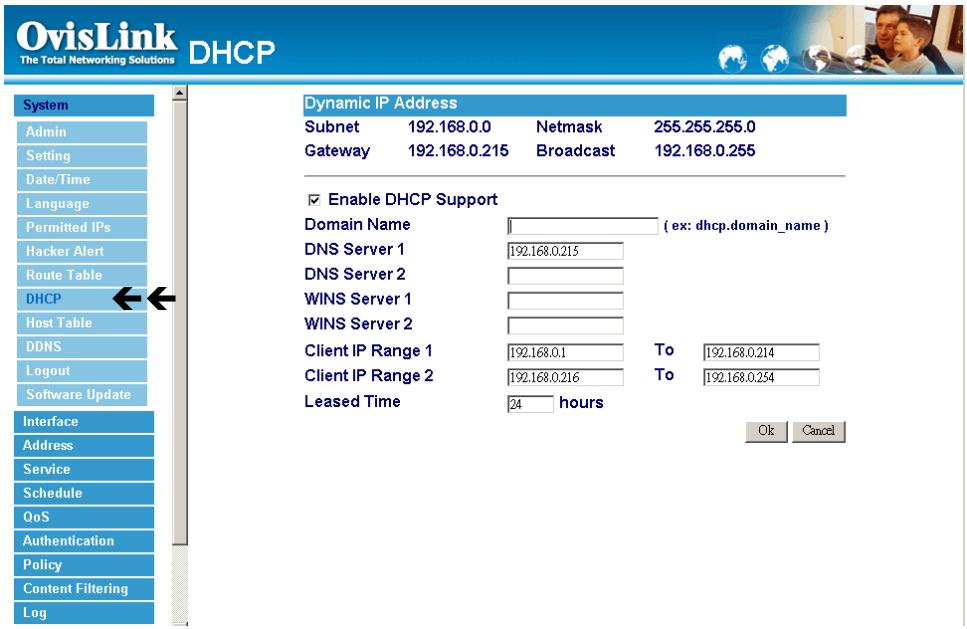


Figure1-29 Dynamic IP address

Dynamic IP Address functions

- **Subnet :** LAN network's subnet
- **NetMask :** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

Enabling DHCP Support

Step 1. In the Dynamic IP Address window, click **Enable DHCP Support**.

Domain Name: The Administrator may enter the name of the LAN network domain if preferred.

DNS Server 1 : Enter the distributed IP address of DNS Server1.

DNS Server 2 : Enter the distributed IP address of DNS Server2.

WINS Server 1 : Enter the distributed IP address of WINS Server1.

WINS Server 2 : Enter the distributed IP address of WINS Server2.

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Step 2. Click **OK** to enable DHCP support.

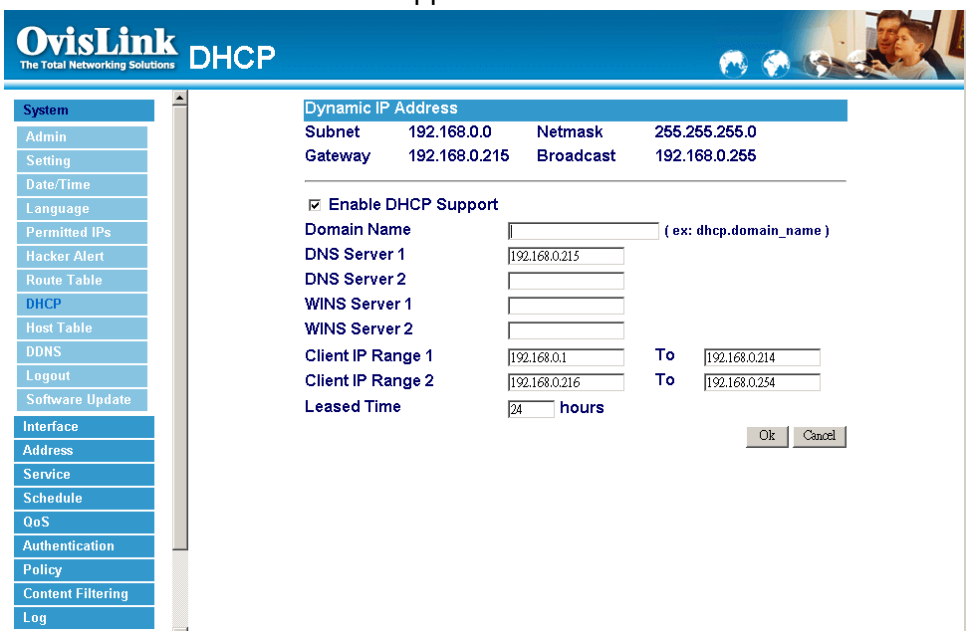


Figure1-30 Enable DHCP Support

Adding a new Host Table

STEP 1． Select **Host Table** in **Settings** function and enter the following setting:

- Click on **New Entry**
- **Host Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address that Host Table mapped to
- Click **OK** and complete adding Host Table. (Figure1-31)

Figure1-31 Add New Host Table WebUI

To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of Bandwidth Manager. That is, the default gateway.

Dynamic DNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.

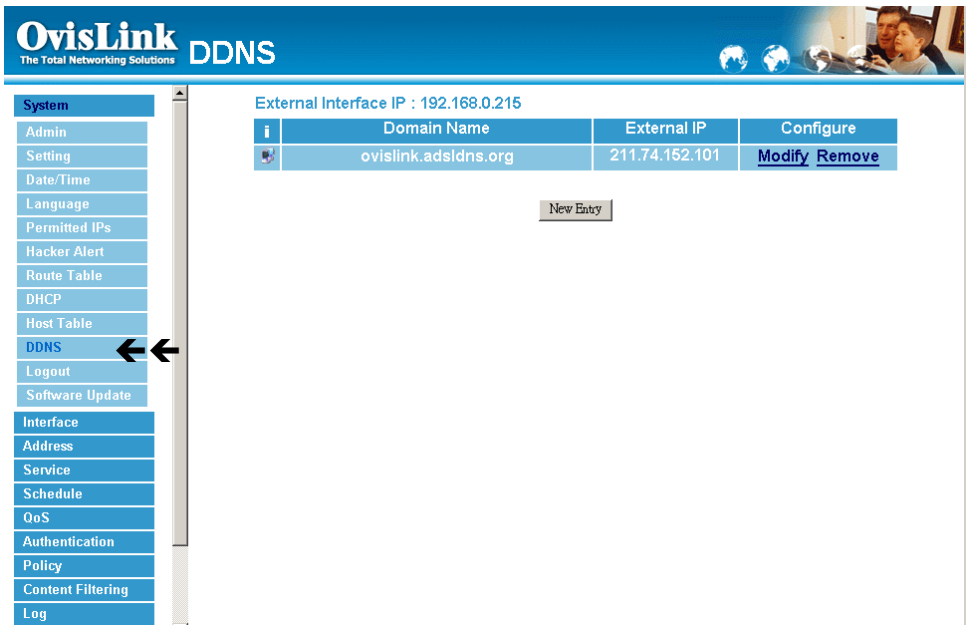


Figure1-31 Dynamic DNS

Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

The nouns in Dynamic DNS window：

!：Update Status【 Connecting; Update succeed; Update fail; Unidentified error**】**

Domain name：Enter the password provided by ISP.

WAN IP Address：IP Address of the WAN port.

Modify: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

How to use dynamic DNS：

The Security Bandwidth Manager provides 3 service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

How to register：Firstly, Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window, then click **Add** button，on the right side of the service providers, click **Register**, the service providers' website will appear, please refer to the website for the way of registration.

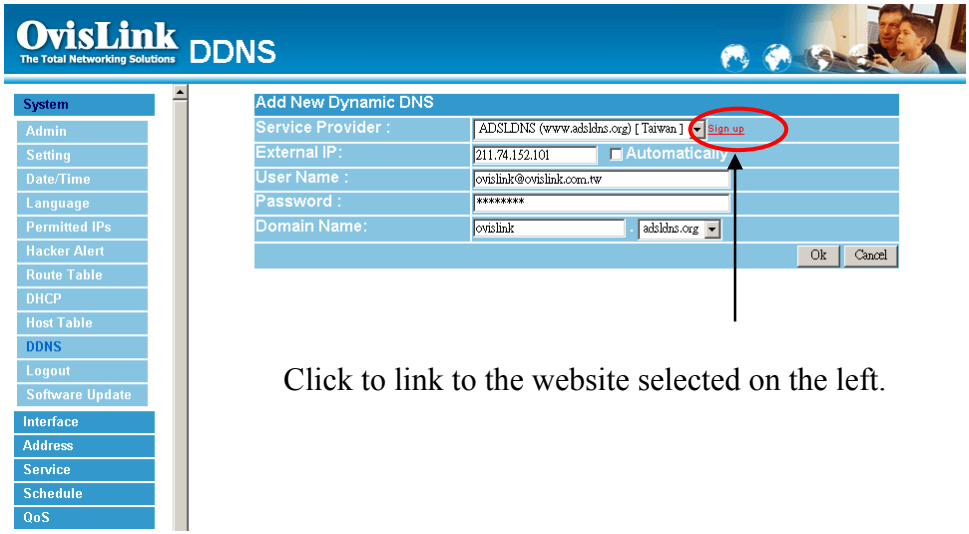


Figure1-32　Setting up DDNS

Add Dynamic DNS settings

Step 1. Click **Add** button.

Step 2. Click the information in the column of the new window.

Service providers：Select service providers.

Register：to the service providers' website.

WAN IP Address：IP Address of the WAN port.

☐ **automatically fill in the WAN IP**：Check to automatically fill in the WAN IP.。

User Name：Enter the registered user name.

Password：Enter the password provided by ISP(Internet Service Provider).

Domain name：Your host domain name provided by ISP.

Click **OK** to add dynamic DNS or click **Cancel** to discard changes.

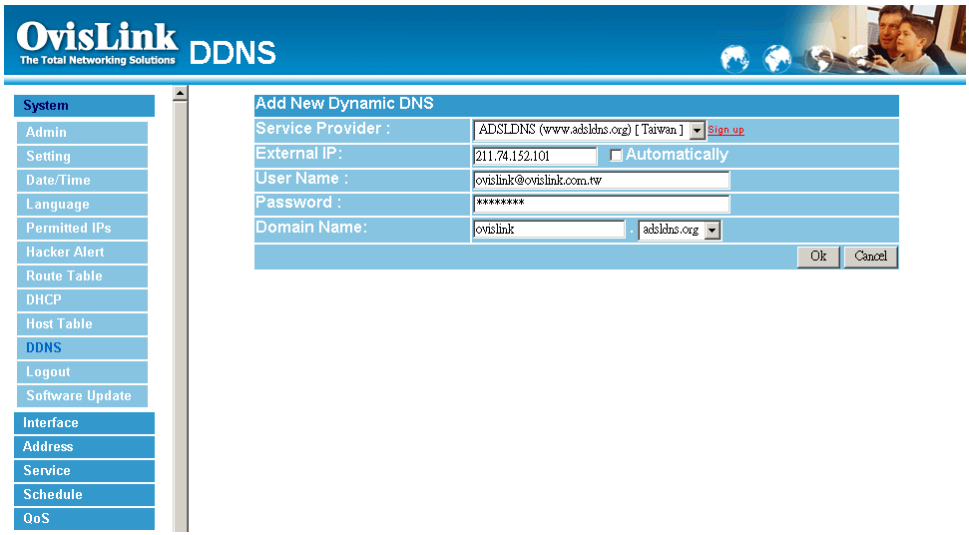


Figure1-33 Add New Dynamic DNS

Modify dynamic DNS

Step 1. Find the item you want to change and click **Modify**.

Step 2. Enter the new information in the Modify Dynamic DNS window.

Click **OK** to change the settings or click **Cancel** to discard changes. ◦

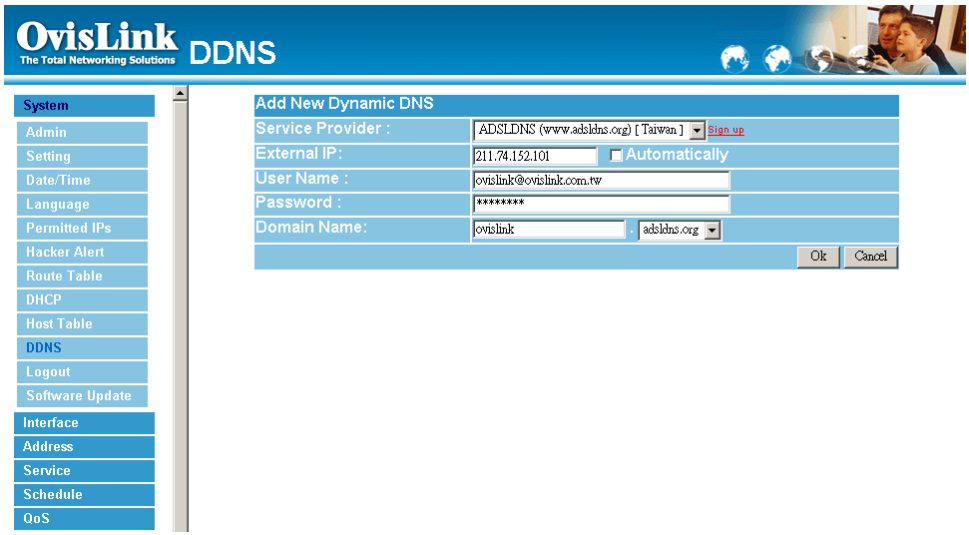


Figure1-34 Modify Dynamic DNS

Delete Dynamic DNS

Step 1. Find the item you want to change and click **Delete**.

Step 2. A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.

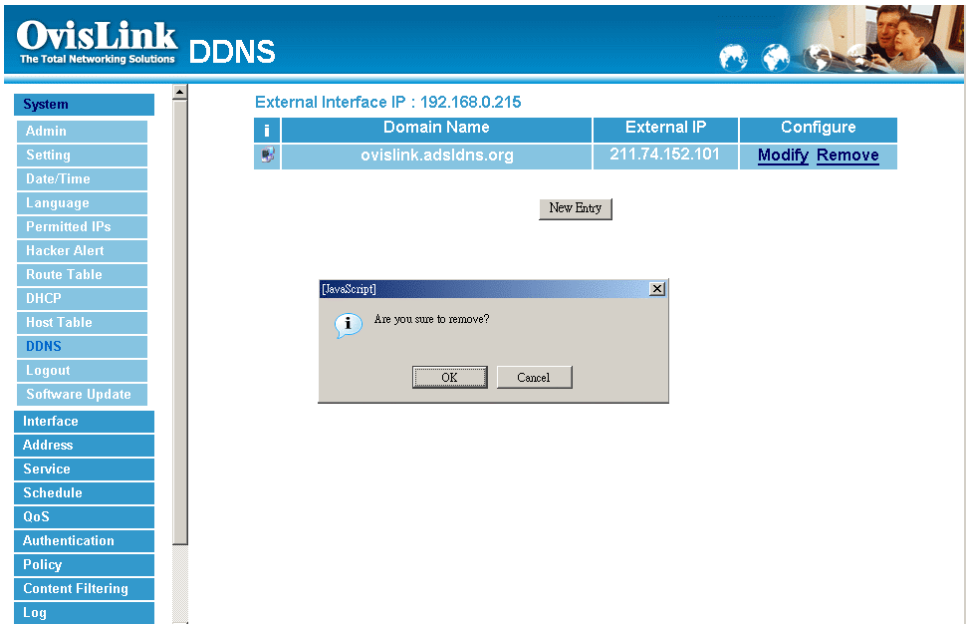


Figure1-35 Remove Dynamic DNS

Logout

Step 1. Select this option to the device's **Logout** the Security Bandwidth Manager. This function protects your system while you are away.

Step 2. Click Logout the Bandwidth Manager.

Step 3. Click **OK** to logout or click **Cancel** to discard the change.

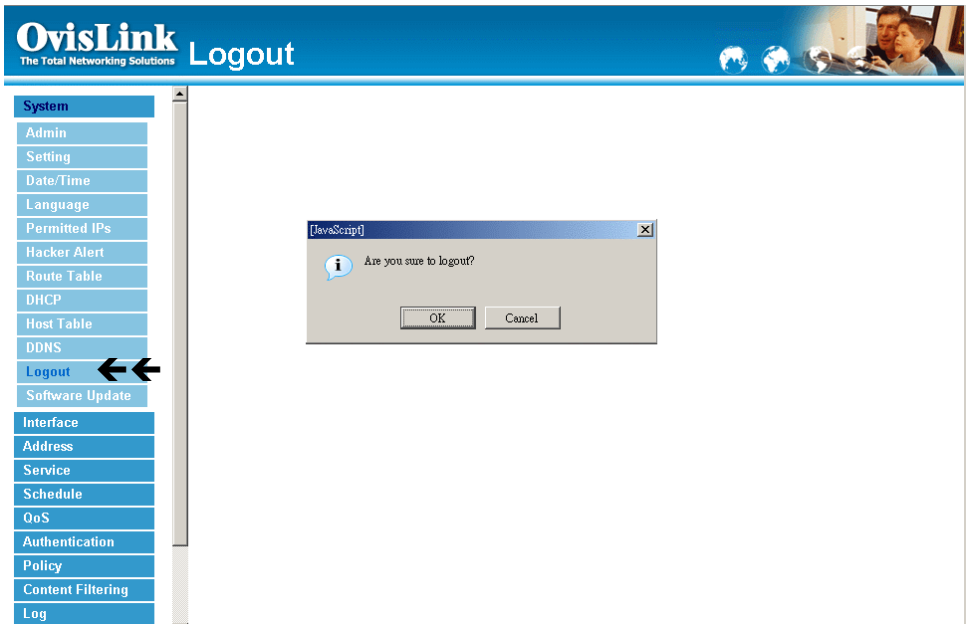


Figure1-36 Logout

Software Update

Under **Software Update**, the admin may update the device's software with a newer software. You may acquire the current version number of software in **Version Number**. Administrators may visit distributor's web site to download the latest version and save it in server's hard disc.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.

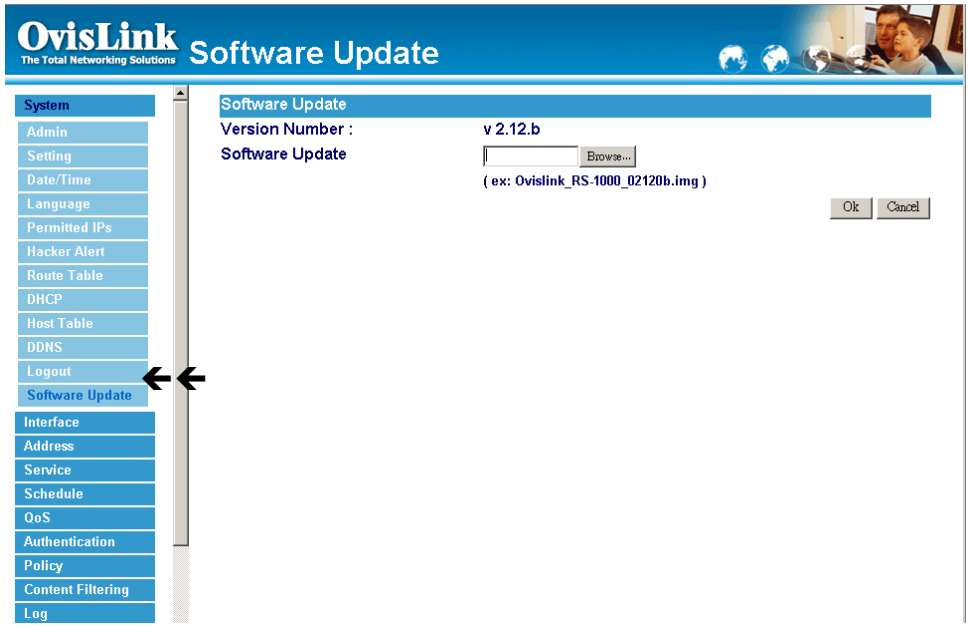


Figure1-37 Software Update

It takes three minutes to update the software. The system will restart automatically after updating the software.

Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the Internal (LAN) network, and the External (WAN) network. The netmask and gateway IP addresses are also configured in this section. In **Interface** section, the **administrator** can configure IP address, Netmask, and Gateway of the LAN network/ WAN network inside the office network, depending on the ISP selected.

Entering the Interface menu:

Step 1. Click on **Configuration** in the left menu bar.

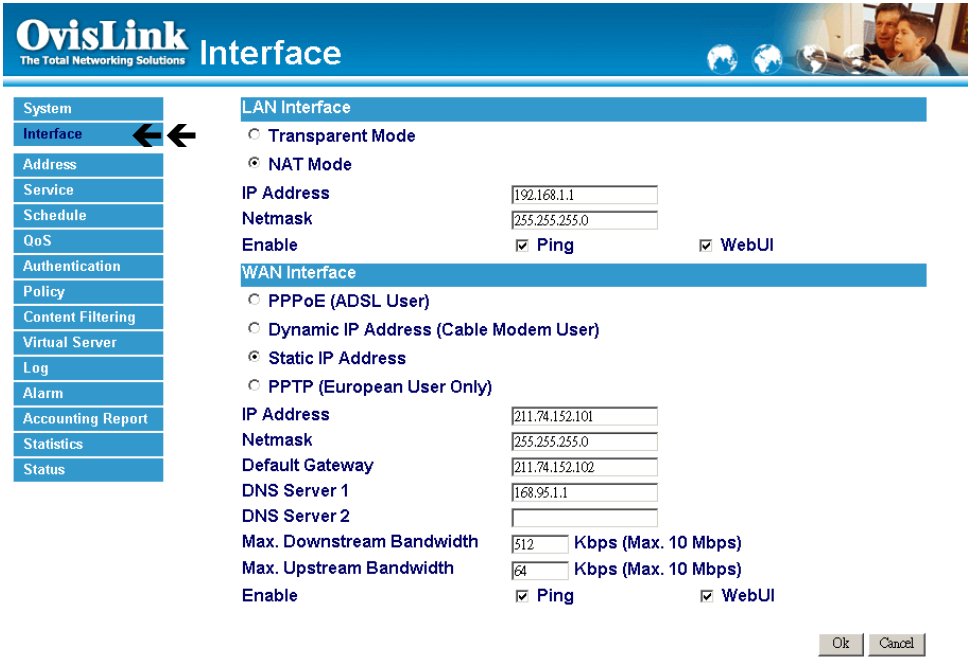
Step 2. Then click on **Interface** below it. The current settings of the interface addresses will appear on the screen.

Internal Interface

Using the Internal Interface, the Administrator sets up the Internal (LAN) network. The Internal network will use a private IP scheme. The private IP network will not be routable on the Internet.

Transparent Mode：All the IP internetwork uses real IP.
NAT Mode：All the IP Internetwork uses NAT (Network Address Translation), which allows the private IP internetworks use non-registered IP addresses to connect to the Internet.

IP Address: The private IP address of the Firewall's internal network is the IP address of the Internal (LAN) port of the Security Bandwidth Manager. The default IP address is 192.168.1.1.
Note:The IP Address of Internal Interface and the DMZ Interface is a private IP address only. If the new Internal IP Address is not 192.168.1.1, the **Administrator** needs to set the IP Address on the computer to be on the same subnet as the Firewall and restart the System to make the new IP address effective. For example, if the Firewall's new Internal IP Address is 172.16.0.1, then enter the new Internal IP Address 172.16.0.1 in the URL field of browser to connect to Firewall.
NetMask: This is the netmask of the internal network. The default netmask of the Security Bandwidth Manager is 255.255.255.0.
Ping: Select this to allow the internal network to ping the IP Address of the Firewall. If set to enable, the Security Bandwidth Manager will respond to ping packets from the internal network.
WebUI: Select this to allow the Security Bandwidth Manager WEBUI to be accessed from the Internal (LAN) network.


OvisLink
The Total Networking Solutions
Interface
System
Interface
Address
Service
Schedule
QoS
Authentication
Policy
Content Filtering
Virtual Server
Log
Alarm
Accounting Report
Statistics
Status
LAN Interface
Transparent Mode
NAT Mode
IP Address 192.168.1.1
Netmask 255.255.255.0
Enable Ping WebUI
WAN Interface
PPPoE (ADSL User)
Dynamic IP Address (Cable Modem User)
Static IP Address
PPTP (European User Only)
IP Address 211.74.152.101
Netmask 255.255.255.0
Default Gateway 211.74.152.102
DNS Server 1 168.95.1.1
DNS Server 2
Max. Downstream Bandwidth 512 Kbps (Max. 10 Mbps)
Max. Upstream Bandwidth 64 Kbps (Max. 10 Mbps)
Enable Ping WebUI
Ok
Cancel

ADSL user Interface setting

PPPoE（External Interface）

Step 1. Select **Interface** function in the menu bar.

Step 2. Check the item **PPPoE (ADSL User)** below **WAN Interface**.

Step 3. Enter each parameter of WAN Interface.

Figure2-2 PPPoE ADSL User Interface

For PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect, such as ADSL users.

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP Address of the PPPoE connection

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Upload/Download Bandwidth：The bandwidth your ISP provided. (Maximum bandwidth for Upload/Download Bandwidth is 10Mbps)

Service-On-Demand:

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. If set to enable, the Security Bandwidth Manager will respond to echo request packets from the external network.

WebUI: Select this to allow the Security Bandwidth Manager WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Security Bandwidth Manager always requires a username and password to enter the WebUI.

After completing the setting, click **OK**.

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by the Firewall from the ISP will be displayed here. This is the IP address of the External (WAN) port of the Security Bandwidth Manager.

MAC Address: This is the MAC Address of the Security Bandwidth Manager.

User Name (Some ISPs may require)：This is provided by your ISP.

Hostname: This will be the name assign to the Security Bandwidth Manager. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP. (Upstream/Downstream can be up to 10Mbps)

Renew: Requests for receiving the new WAN IP address.

Release: Requests for releasing the obtained WAN IP address.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. *If set to enable, the* Security Bandwidth Manager *will respond to echo request packets from the external network.*

WebUI: Select this to allow the Security Bandwidth Manager WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Security Bandwidth Manager always requires a username and password to enter the WebUI.

After setting all of the parameters, click **OK** button.

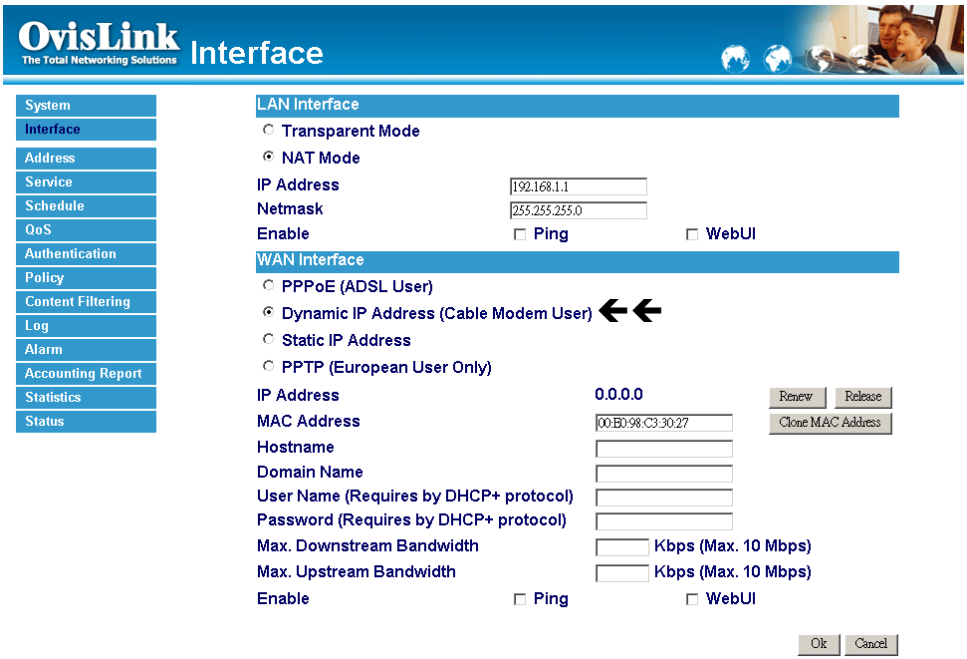


Figure2-3 Dynamic IP Address (Cable Modem User)

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the External (WAN) port of the Security Bandwidth Manager.

Netmask: This will be the Netmask of the external (WAN) network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

DNS Server 1/2: Enter the DNS 1/2 server provided by ISP. (See *Note.)*

Max. Upstream Bandwidth/Max. Downstream Bandwidth: The bandwidth provided by ISP. (Upstream/Downstream can be up to 10Mbps)

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. *If set to enable, the* Security Bandwidth Manager *will respond to echo request packets from the external network.*

WebUI: Select this to allow the Security Bandwidth Manager WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Security Bandwidth Manager always requires a username and password to enter the WebUI.

After setting all of the interface address, click **OK** button.

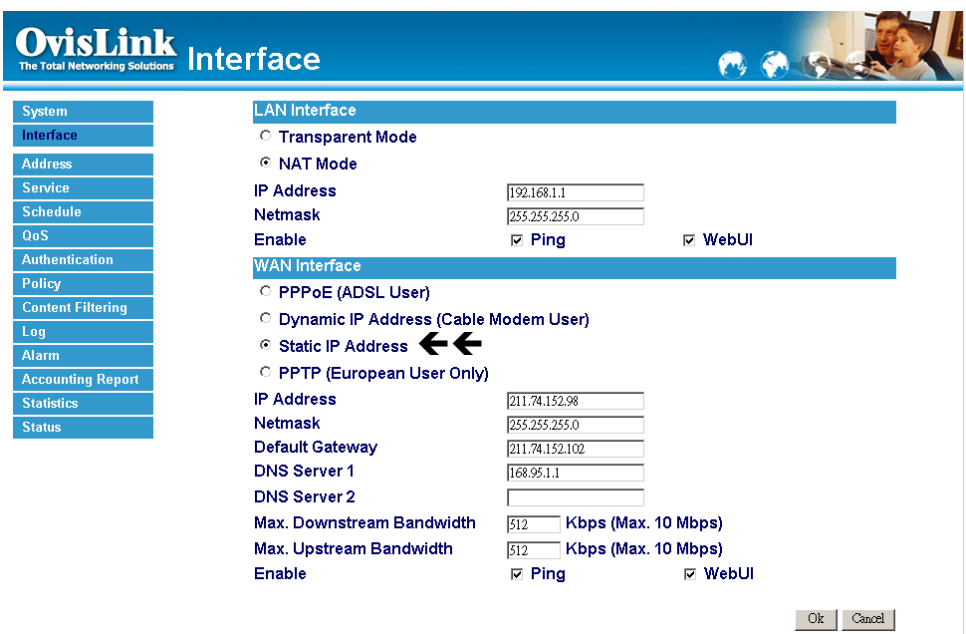


Figure2-4 WAN interface setup for Static IP Address

If you want to set up DNS Server, you have to go to **Virtual Server** function to map the real IP address from DNS server to the corresponding private IP address of internal DNS server. Enter the mapped IP address of internal server in DNS server address field.

For PPTP (European User Only): This option is for PPTP users who are required to enter a username and password in order to connect, especially for European Users.

Current Status: Displays the current line status of the PPTP connection.

IP Address: Displays the IP Address of the PPTP connection

Username: Enter the PPTP username provided by the ISP.

Password: Enter the PPTP password provided by the ISP.

Local IP: Select To obtain an IP address automatically or Use the following IP address.

MAC Address: This is the MAC Address of the Bandwidth Manager.

Hostname: This will be the name assign to the Bandwidth Manager. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: This will be the domain name assign to the Bandwidth Manager.

IP Address: Enter the IP address assigned to you by your ISP. This will be the public IP address of the External (WAN) port of the Bandwidth Manager.

Netmask: This will be the Netmask of the external (WAN) network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

PPTP Gateway: This will be the PPTP Server IP address.

Connect ID: Enter the phone number that provided and asked by some ISP. (Optional)

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP. (Upstream/Downstream can be up to 10Mbps)

BEZEQ-ISRAEL: The selection especially for the user who wants to connect to Bezeq (the Israeli phone company which doesn't conform to the RFC protocol).

Service-On-Demand:

Auto Disconnect: The PPTP connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPTP connection to disconnect at all.

Address

The Security Bandwidth Manager allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN network, WAN group.

What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address . If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN **Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.
With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

How to use Address Table

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

LAN

Entering the LAN window

Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.

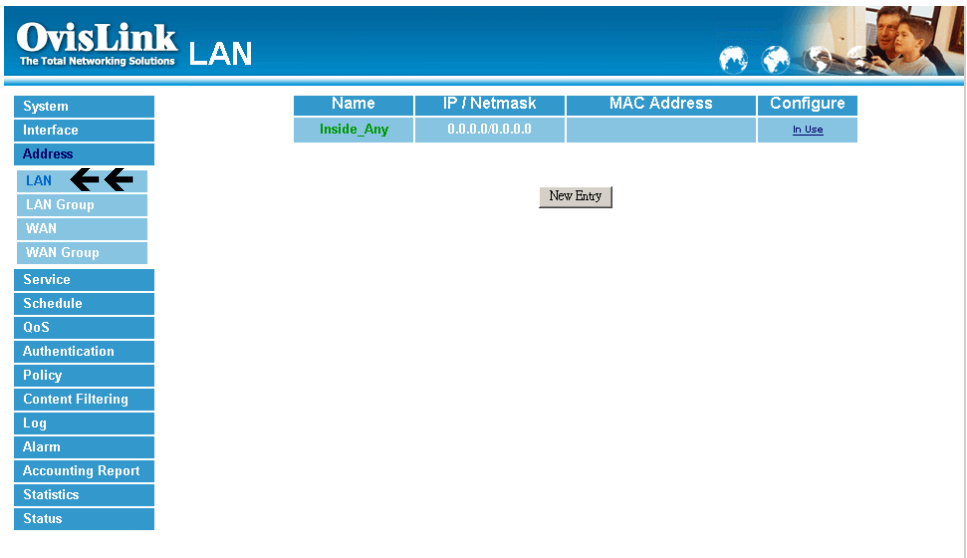


Figure3-1 LAN

Definition

Name: Name of LAN network address.

IP：IP address of LAN network

Netmask: Netmask of LAN network.

MAC Address: MAC address corresponded with LAN IP address.

Configure: You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN network. Click **Remove** to delete the settings.

In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

Adding a new LAN Address

Step 1. In the LAN window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.

Step 3. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.

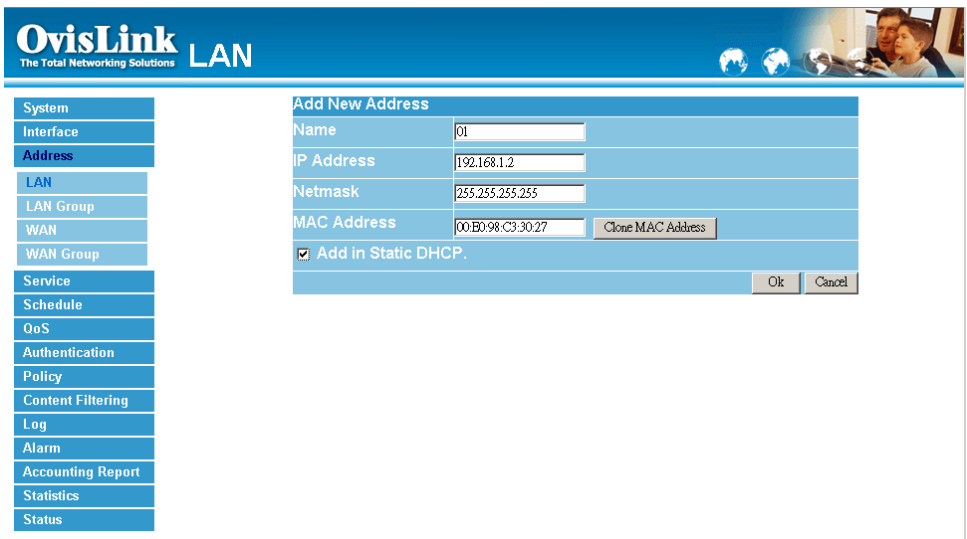


Figure3-2 Add New IP Address in LAN

If you want to enable **Add in Static DHCP** function, enter the MAC Address then check the **Add in Static DHCP**.

Modifying an LAN Address

Step 1. In the LAN window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.

Step 2. In the **Modify Address** window, fill in the new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

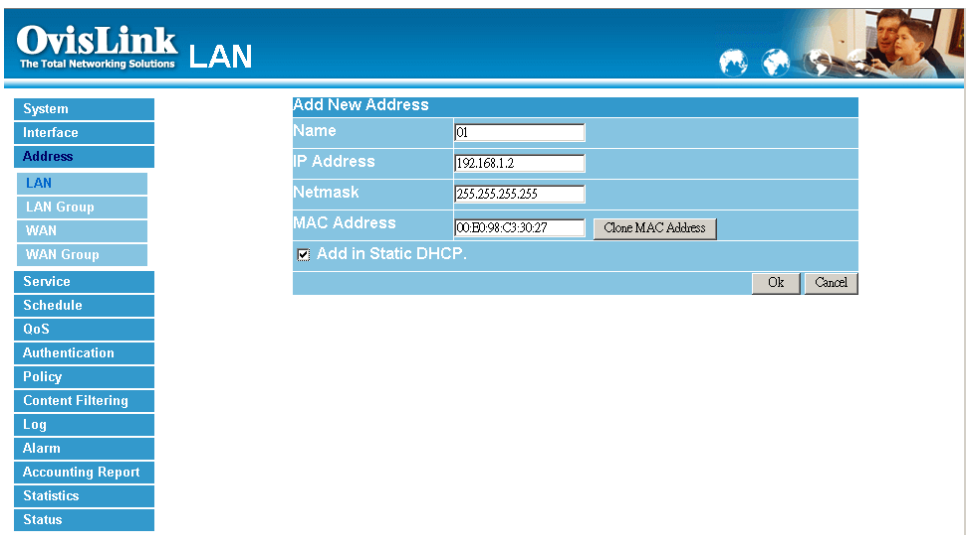


Figure3-3 Modify LAN IP Address

Removing a LAN Address

Step 1. In the LAN window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

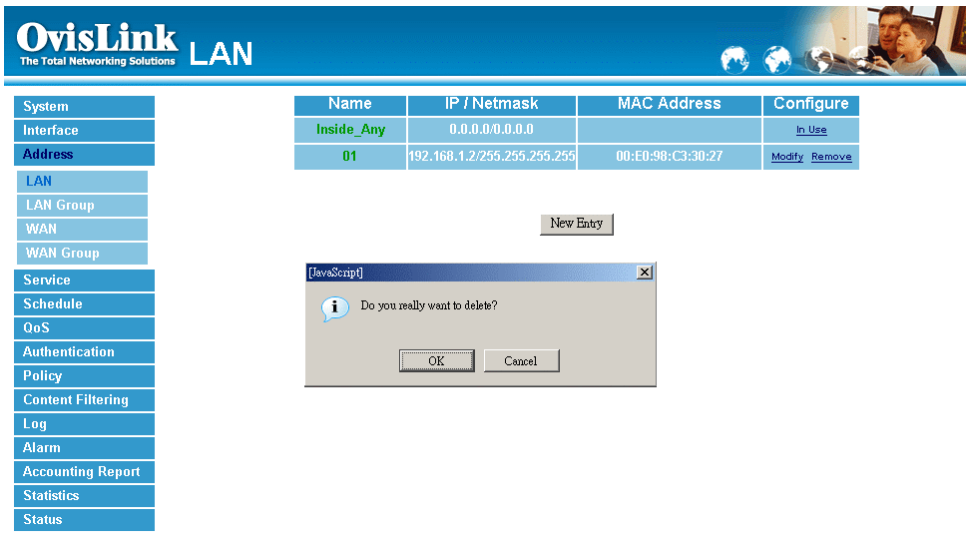


Figure3-4 Remove LAN IP Addresses

LAN Group

Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

Step 1. Click LAN **Group** under the **Address** menu to enter the LAN Group window. The current setting information for the LAN network group appears on the screen.

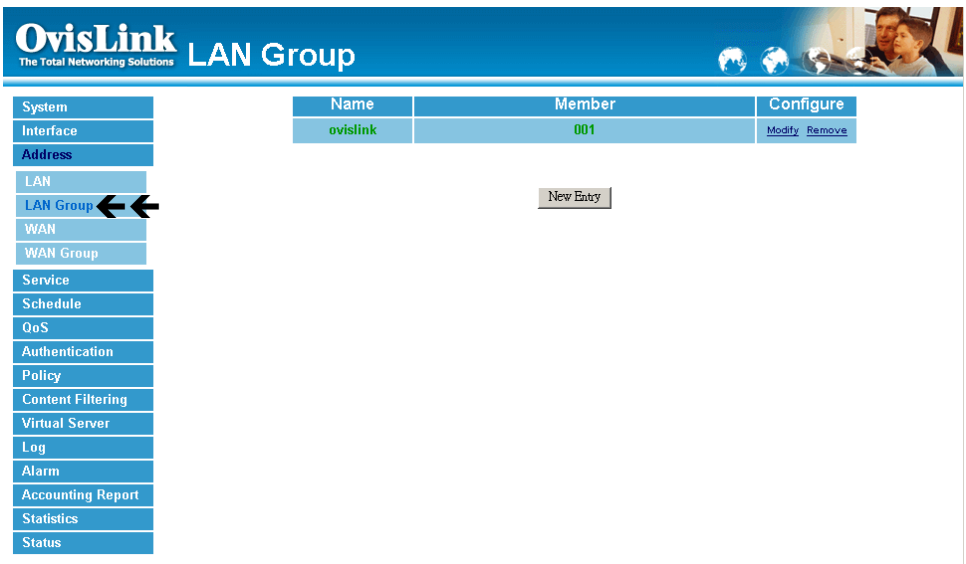


Figure3-5 LAN Group

Definitions (LAN group):

Name: Name of the LAN group.

Member: Members of the group.

Configure: Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click **Remove** to delete the group.

In the **LAN Group** window, if one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group. You have to delete the Group in **Policy** window, and then you are allowed to configure the LAN Group.

Adding a LAN Group

Step 1. In the LAN **Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

Step 2. In the Add New Address Group window:

- **Available Address:** list the names of all the members of the LAN network.
- **Selected Address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available Address list, and click the **Add>>** button to add them to the Selected Address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click Cancel to discard changes.

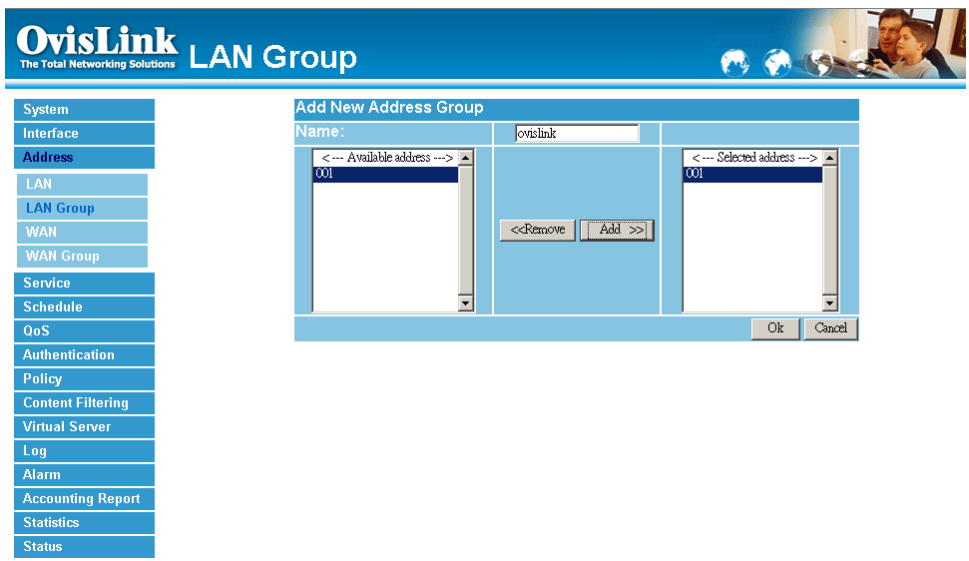


Figure3-6 Add New LAN Group

Modifying a LAN Group

Step 1. In the LAN **Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list names of all members of the LAN network.
- **Selected Address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names in the **Selected Address** list, and click the **<<Remove** button to remove these members from the **Selected Address** list.

Click **OK** to save changes or click **Cancel** to discard changes.

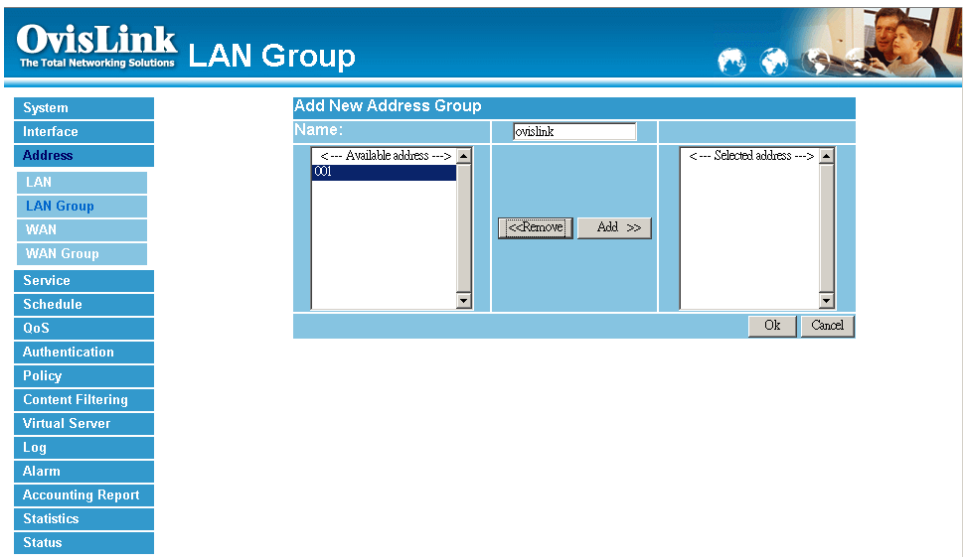


Figure3-7 Modify LAN Group

Removing a LAN Group

Step 1. In the LAN **Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

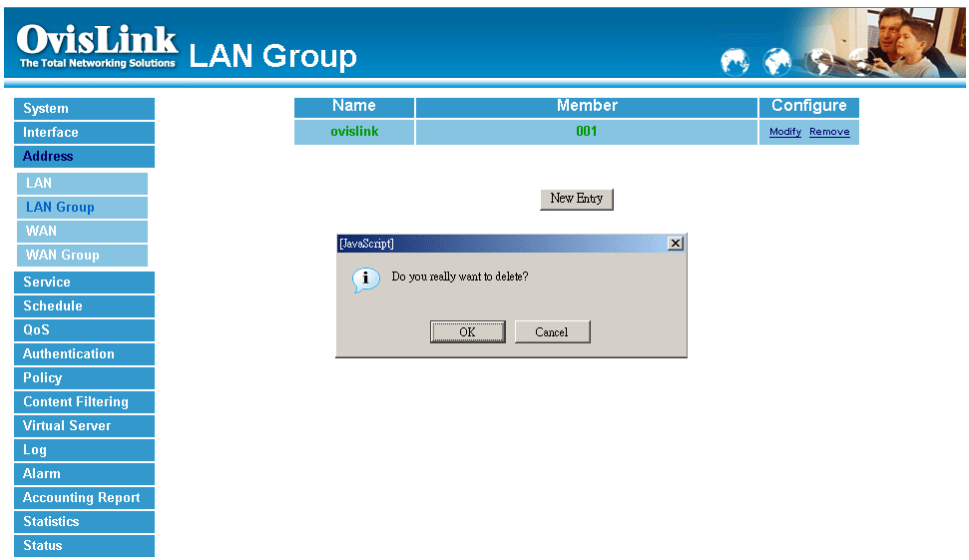


Figure 3-8 Remove LAN Group

WAN

Entering the WAN window

Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.

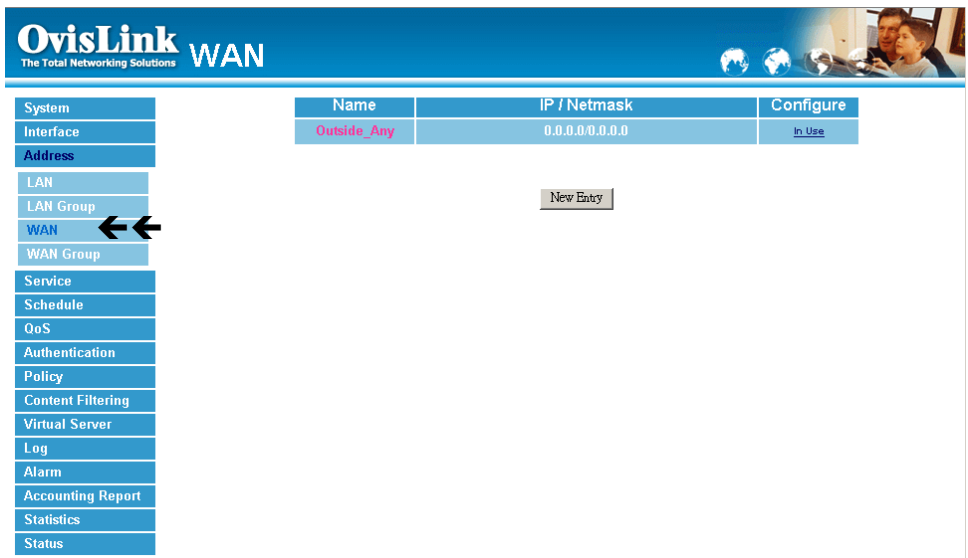


Figure3-9 WAN

Definitions

Name: Name of WAN network address.

IP/Netmask: IP address/Netmask of WAN network.

Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network. Click **Remove** to delete the setting of WAN network.

In the WAN Network window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.

Adding a new WAN Address

Step 1. In the WAN window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.

Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.

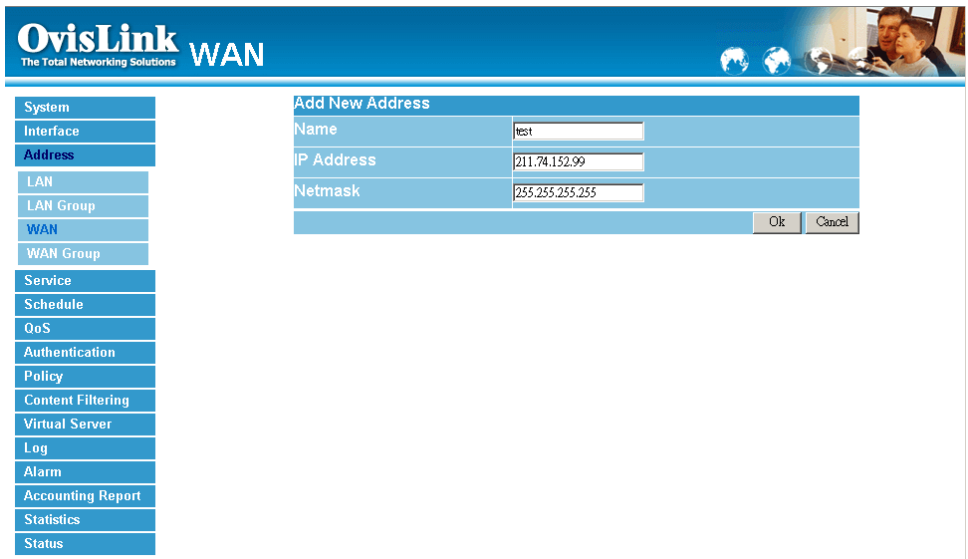


Figure3-10 Add WAN IP Address

Modifying an WAN Address

Step 1. In the WAN table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

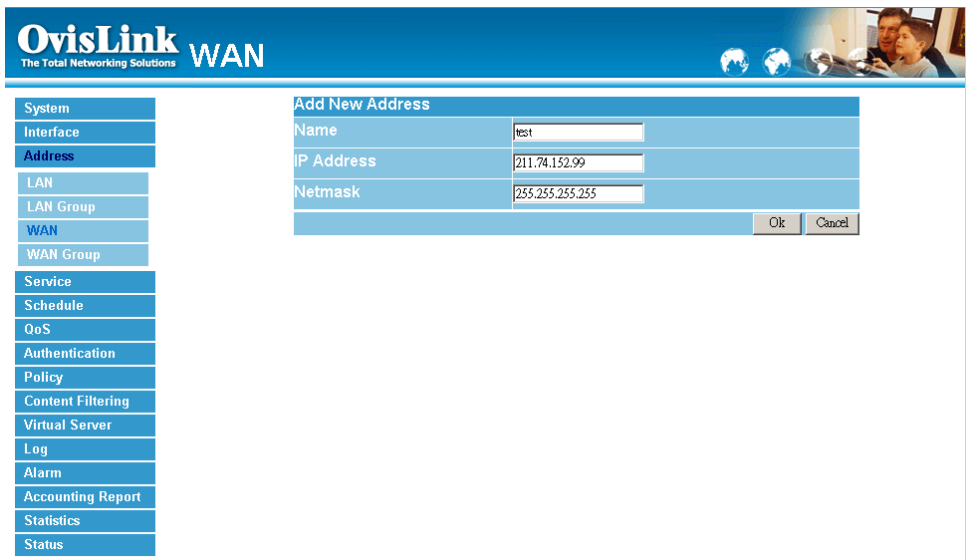


Figure3-11 Modify WAN IP Address

Removing an WAN Address

Step 1. In the WAN table, locate the name of the network to be removed and click the **Remove** option in its corresponding Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

Figure3-12 Remove a WAN IP address

WAN Group

Entering the WAN Group window

Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current settings for the WAN network group(s) will appear on the screen.

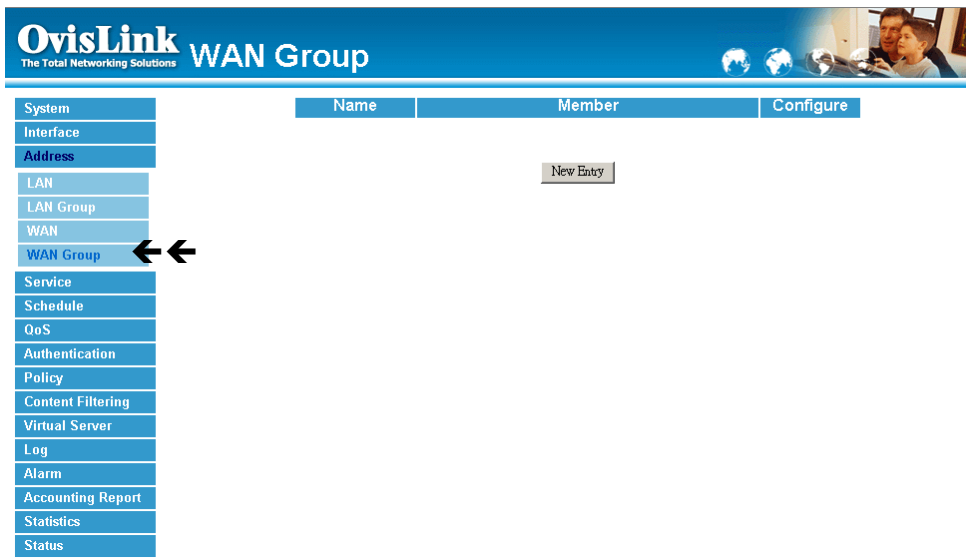


Figure3-13 WAN Group

Definitions:

Name: Name of the WAN group.

Member: Members of the group.

Configure: Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group Click Remove to delete the selected group.

*In the **WAN Group** window, if one of the members has been added to the **Policy**, "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the **Policy** window to remove the setting, and then you can configure.*

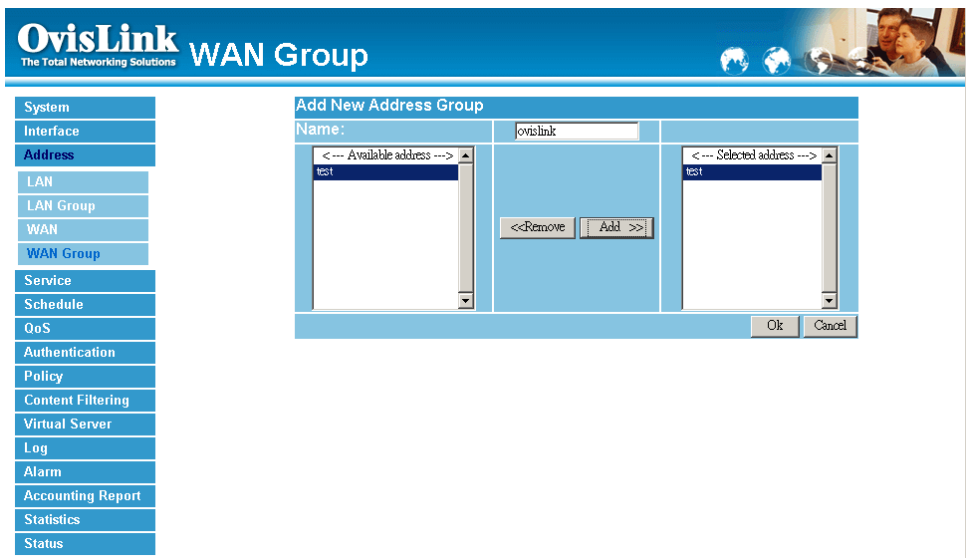
Adding an WAN Group

Step 1. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 2. In the **Add New Address Group** window the following fields will appear:

- **Name:** enter the name of the new group.
- **Available Address:** List the names of all the members of the WAN network.
- **Selected Address:** List the names to assign to the new group.
- **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.
- **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.



3-14 Add a new WAN Group

Modifying a WAN Group

Step 1. In the **WAN Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.

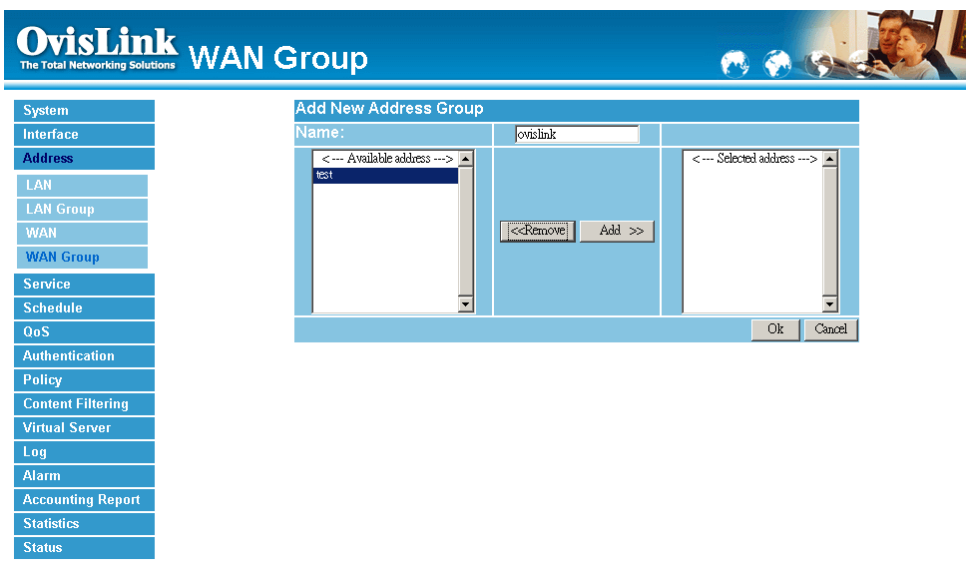
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list the names of all the members of the WAN network.
- **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.



3-15 Modify a WAN Group

Removing a WAN Group

Step 1. In the **WAN Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

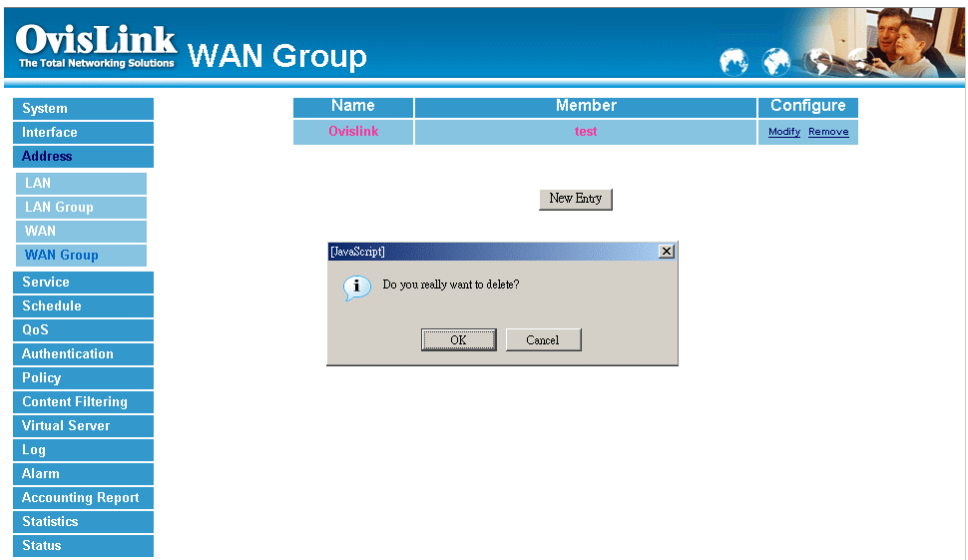


Figure 3-16 Remove WAN Group

Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined**, **Custom**, and **Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. The Security Bandwidth Manager defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

How do I use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

Pre-defined

Entering a Pre-defined window

Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.

Figure4-1 Pre-defined Service

Icons and Descriptions

Figu	Description
TCP	TCP services, i.g. FTP、FINGER、HTTP、、HTTPS 、IMAP、SMTP、POP3、ANY、AOL、BGP、GOPHER、InterLocator、IRC、L2TP、LDAP、NetMeeting、NNTP、PPTPReal、 Media、RLOGIN、SSH、TCP ANY、TELNET、VDO Live、WAIS、WINFRAME、
UDP	UDP services, i.g. IKE、DNS、NTP、IRC、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-ANY、UUC, etc.
ICMP	ICMP services, i.g. PING、TRACEROUTE, etc.

Custom

Entering the Custom window

Step 1. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.

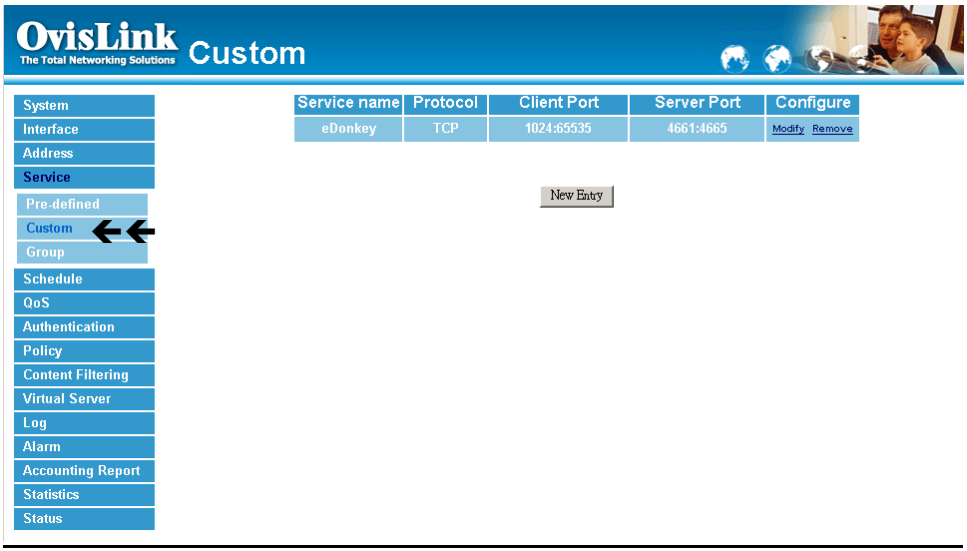


Figure4-2 Custom Service

Definitions:

Service name: The defined service name.

Protocol: Network protocol used in the basic setting. Such as TCP、UDP or others.

Client port: The range of Client port in defined service.

If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

Service port: The range of Service port in defined service.

If the number of ports entered in the two fields of Service port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Service port is identical, it means that the entered port number is opened.

Configure: Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.

*Note: In the **Custom** window, if one of the services has been added to **Policy** or **Group**, "**In***

***Use**" message will appear in the **Configure** column. In this case you are not allowed to modify or remove the settings. Go to the **Policy** or **Group** window to delete the setting, and then you can configure the settings*.

Adding a new Service

In the **Custom** window, click the **New Entry** button and a new service table appears.
In the new service table:

- New Service Name: This will be the name referencing the new service.
- Protocol: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- Client Port: enter the range of port number of new clients.
- Server Port: enter the range of port number of new servers.

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

Step 1. Click **OK** to add new services, or click **Cancel** to cancel.

Step 2. Click **OK** to accept editing; or click **Cancel**.

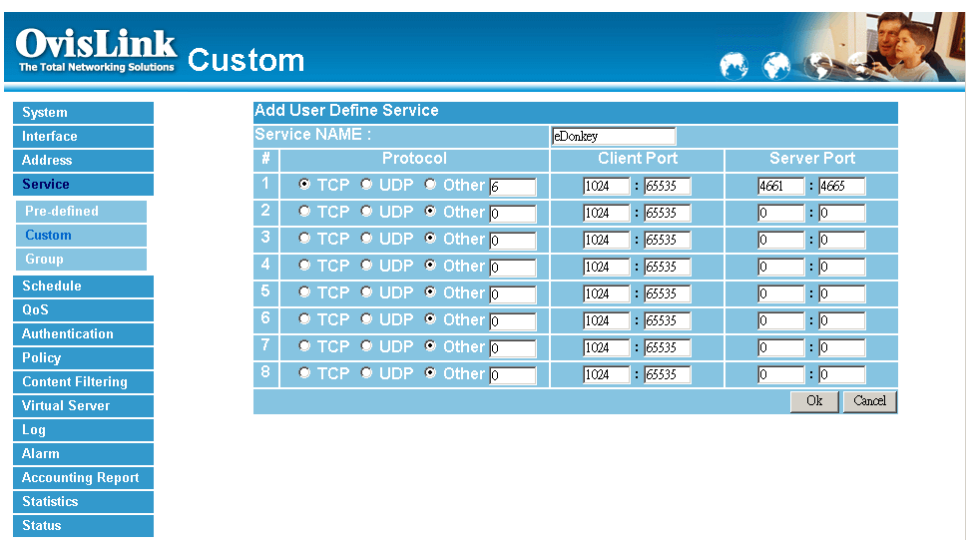


Figure4-3 Add New Custom Service

Modifying Custom Services

Step 1. A table showing the current settings of the selected service appears on the screen

Step 2. Enter the new values.

Step 3. Click **OK** to accept editing; or click **Cancel**.

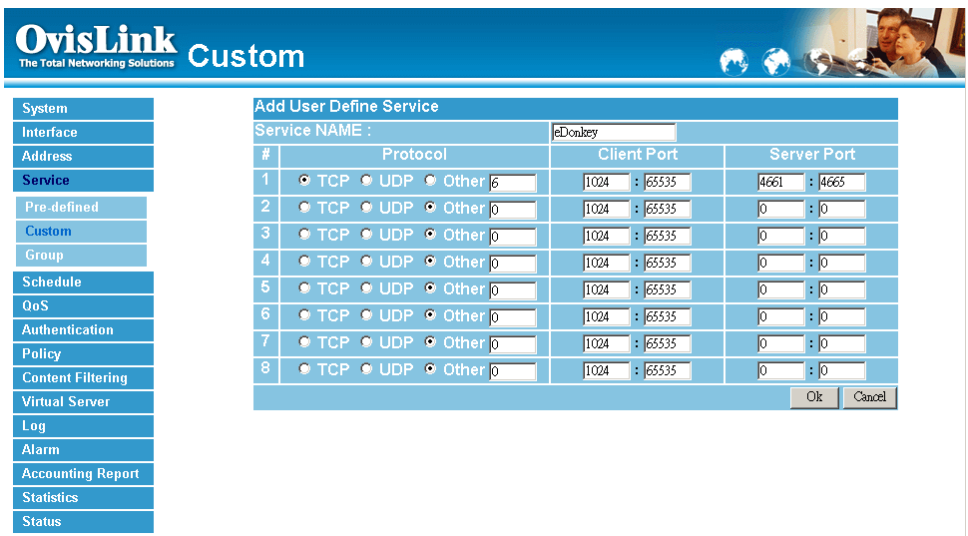


Figure4-4 Modify Custom Service

Removing Custom Services

Step 1. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.

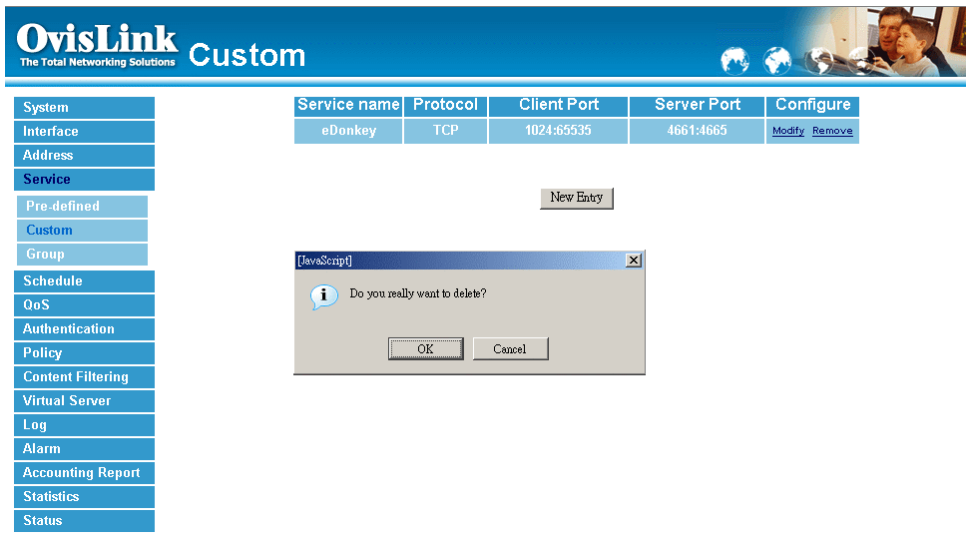


Figure4-5 Remove Custom Service

Group

Accessing the Group window

Step 1. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.

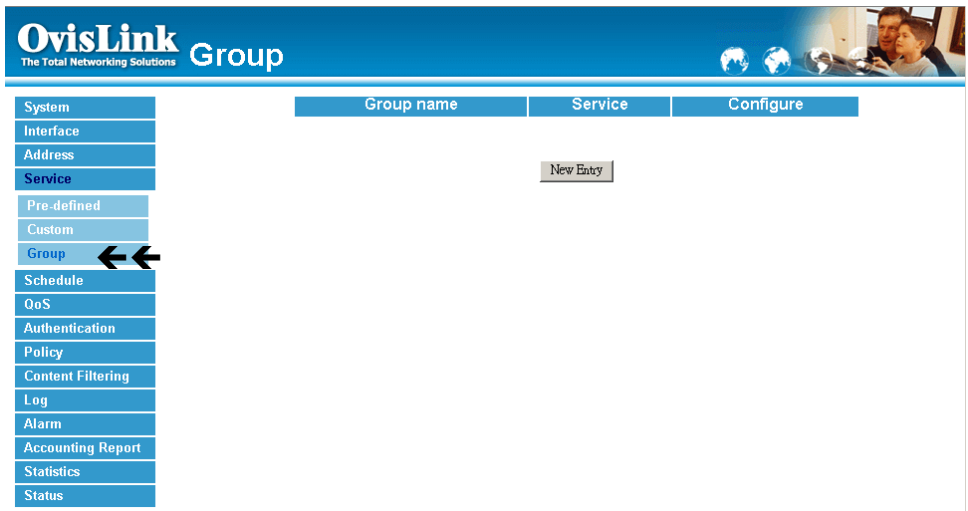


Figure4-6 Service Group

Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

Configure: Configure the settings of Group. Click **Modify** to change the parameters of the Group. Click Remove to delete the Group.

In the **Group** window, if one of the Service Groups has been added to **Policy**. "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the Policy window, remove the Service group first, and then you are allowed to configure the setting.

Adding Service Groups

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

- **Available Services:** list all the available services.
- **Selected Services:** list services to be assigned to the new group.

Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available Services** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Available Services**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.

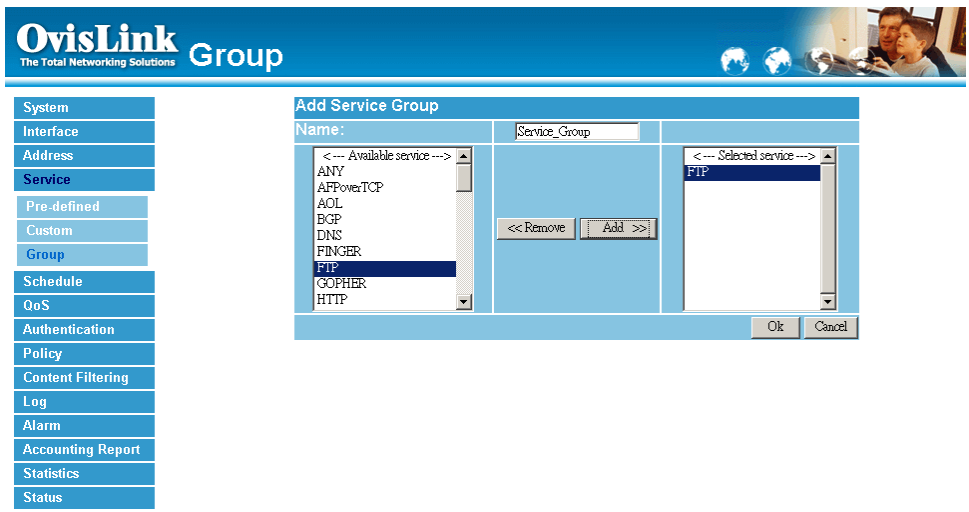


Figure4-7 Add New Group

Modifying Service Groups

Step 1. In the Mod (modify) group window the following fields are displayed:

- **Available Services:** lists all the available services.
- **Selected Services:** list services that have been assigned to the selected group.

Step 2. **Add new services:** Select services in the **Available Services** list, and then click the **Add>>** button to add them to the group.

Step 3. **Remove services:** Select services to be removed in the **Selected Services** list, and then click the **<<Remove** button to remove theses services from the group.

Step 4. Click **OK** to save editing changes.

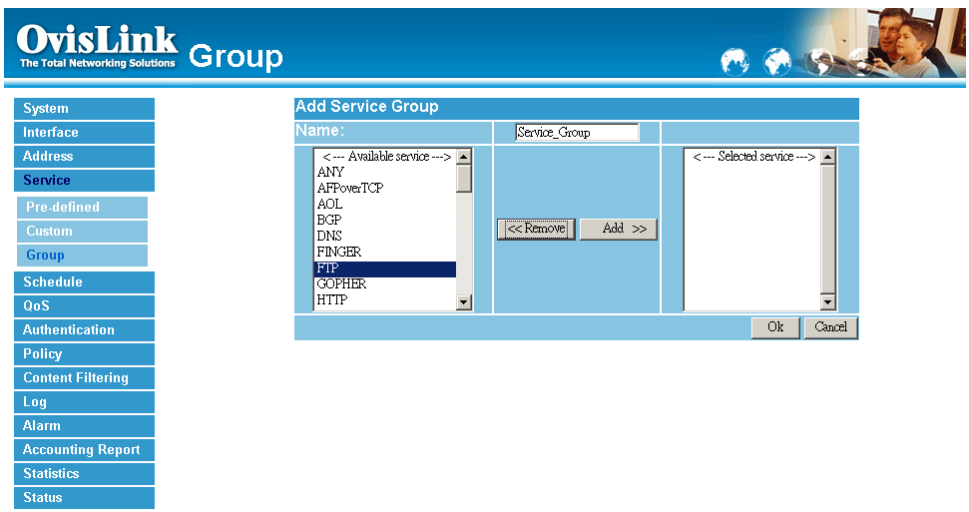


Figure4-8 Modify Group

Removing Service Groups

In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.

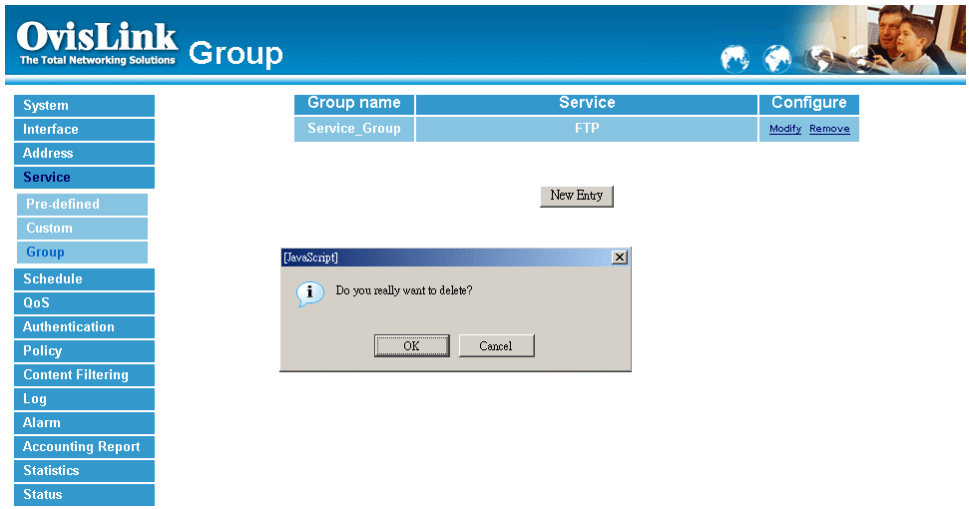


Figure4-9 Remove Group

Schedule

The Security Bandwidth Manager allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Security Bandwidth Manager policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Security Bandwidth Manager policies therefore will likely not be permitted to pass through the Security Bandwidth Manager. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Security Bandwidth Manager to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Security Bandwidth Manager to work Monday-Friday, 8AM-5PM only. During the non-work hours, the Security Bandwidth Manager will not allow Internet access.

Accessing the Schedule window

Step 1. Click on **Schedule** on the menu bar and the schedule window will appear displaying the active schedules.

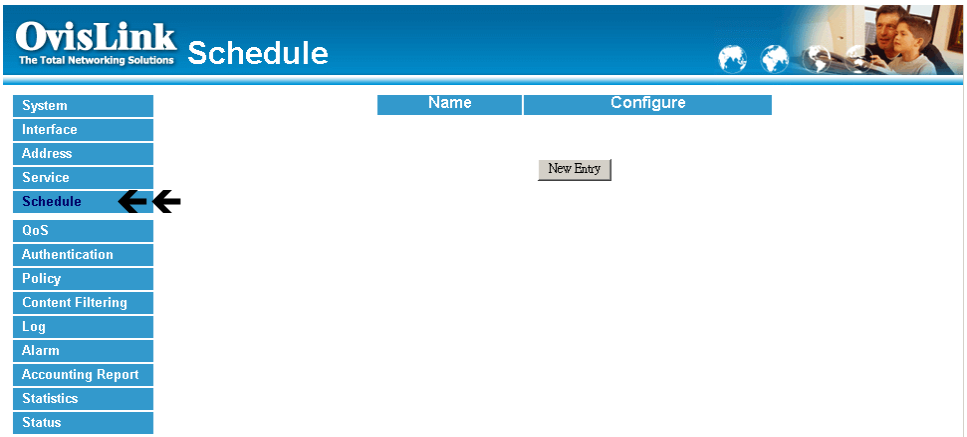


Figure5-1 Schedule

The following items are displayed in this window:

Name: the name assigned to the schedule

Comment: a short comment describing the schedule

Configure: modify or remove

Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

- **Schedule Name:** Fill in a name for the new schedule.
- **Period 1:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click Cancel to cancel adding the new schedule.

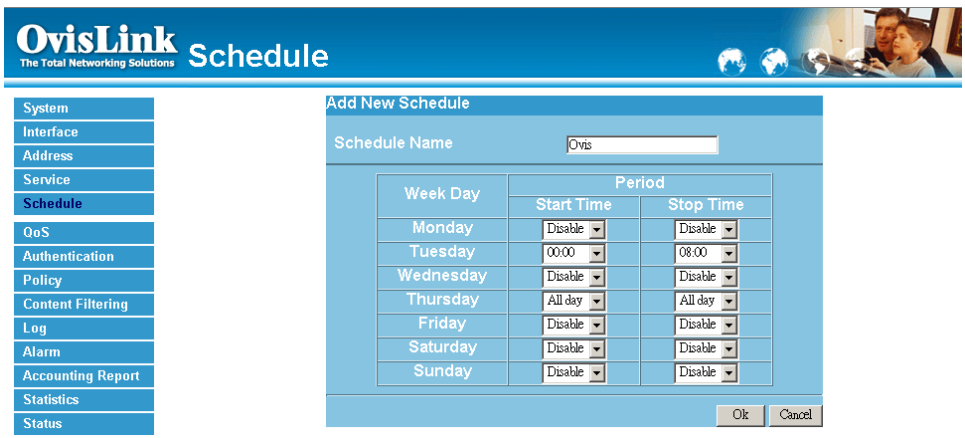


Figure5-2 Add New Schedule

In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

Modifying a Schedule

Step 1. In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field. Make needed changes.

Step 2. Click **OK** to save changes.

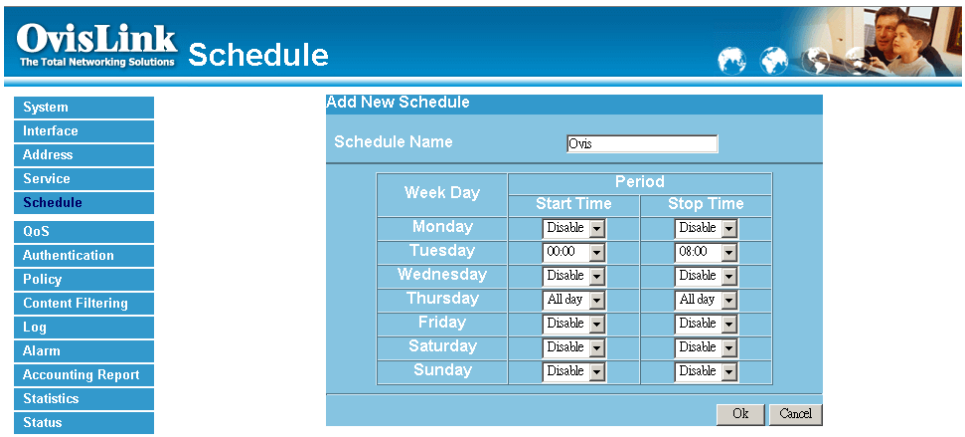


Figure5-3 Modify Schedule

Removing a Schedule

Step 1. In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the schedule.

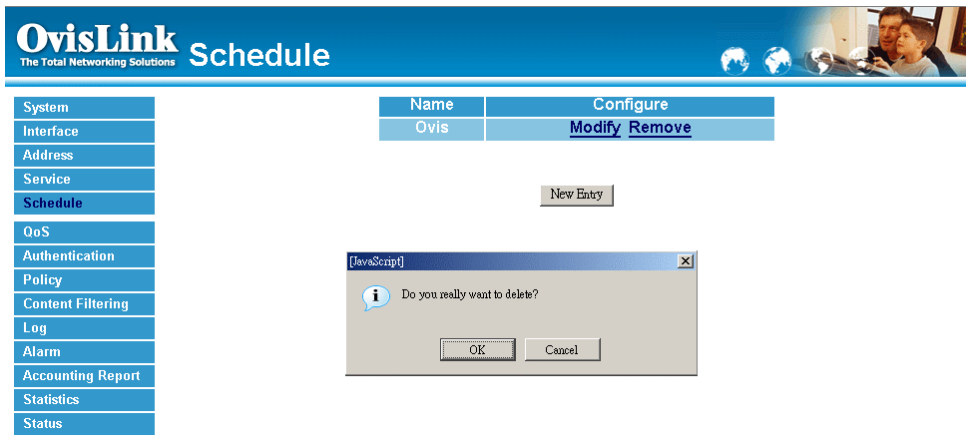


Figure5-4 Remove Schedule

QoS

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth.

Downstream Bandwidth： To configure the Guaranteed Bandwidth and Maximum Bandwidth.

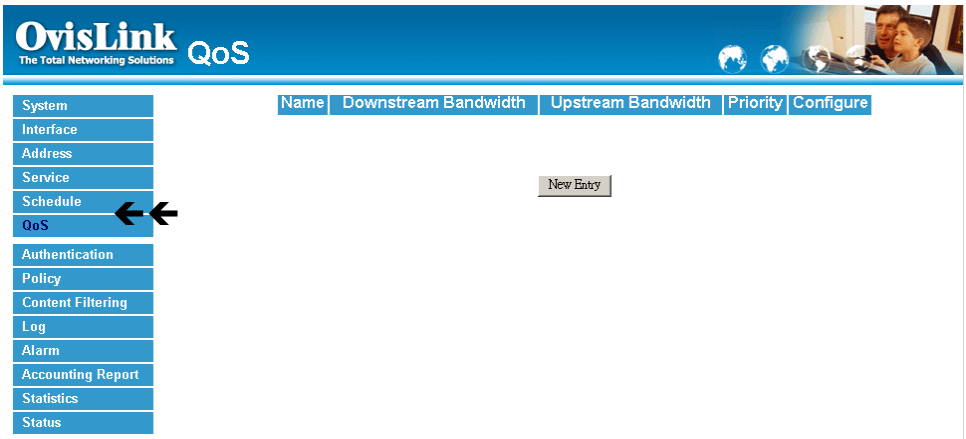
Upstream Bandwidth： To configure the Guaranteed Bandwidth and Maximum Bandwidth.

QoS Priority：To configure the priority of distributing Upstream/Downstream and unused bandwidth.

The Security Bandwidth Manager configures the bandwidth by different QoS , and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The Security Bandwidth Manager also makes it convenient for the administrator to use the Security Bandwidth Manager with the best Utility.

Configuration of QoS

Click QoS in the menu bar on the left hand side.



Definitions:

Name：The name of the QoS you want to configure.

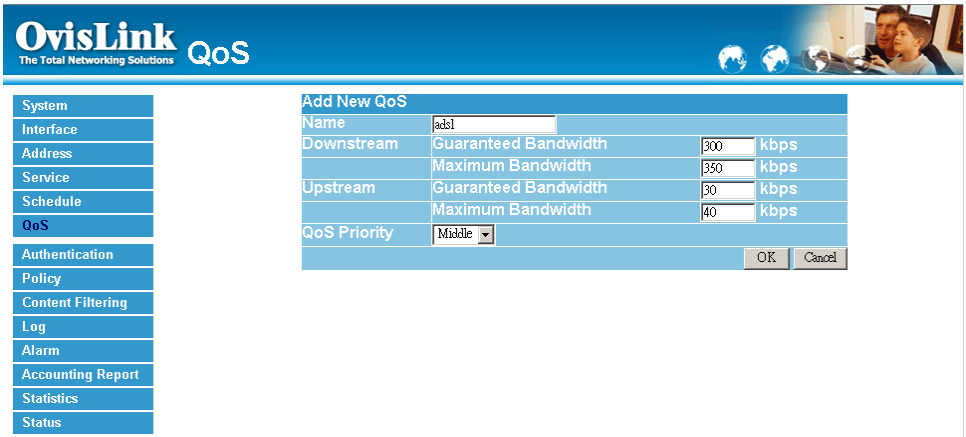
Downstream Bandwidth：To configure the Guarateed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth：To configure the Guarateed Bandwidth and Maximum Bandwidth.

QoS Priority：To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Add New QoS

Step 1. Click QoS in the menu bar on the left hand side.



Step 2. Click the **New Entry** button to add new QoS.

Definition

Name：The name of the QoS you want to configure.

Downstream Bandwidth：**To configure the Guarateed Bandwidth and Maximum Bandwidth.**

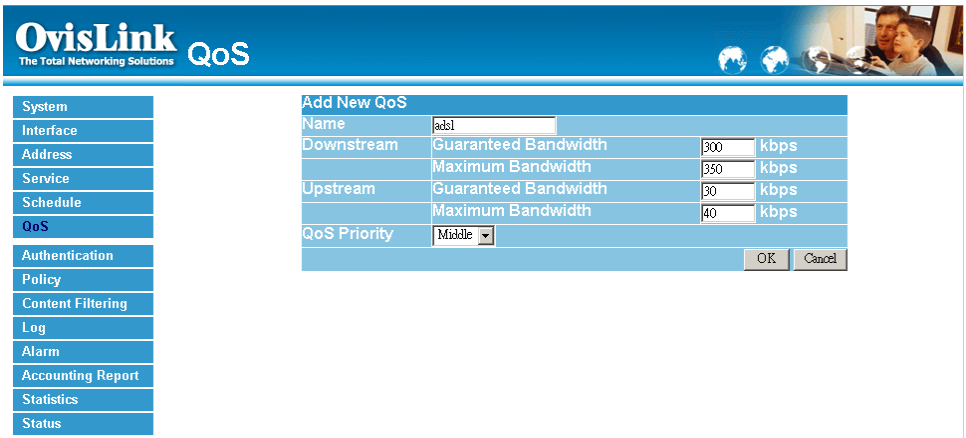
Upstream Bandwidth：**To configure the Guarateed Bandwidth and Maximum Bandwidth.**

QoS Priority：**To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.**

Click the **OK** button to add new QoS.

Modify QoS

Step 1. Click QoS in the menu bar on the left hand side.



Click the Modify button to modify QoS.

Definition:

Name：The name of the QoS you want to configure.

Downstream Bandwidth：**To configure the Guarateed Bandwidth and Maximum Bandwidth.**

Upstream Bandwidth：**To configure the Guarateed Bandwidth and Maximum Bandwidth.**

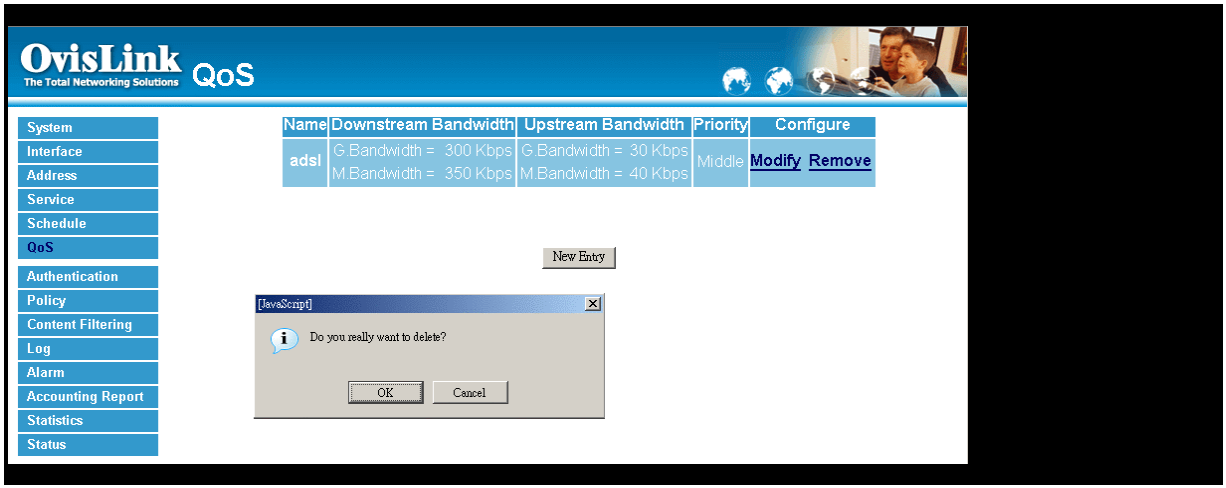
QoS Priority：**To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.**

Click the **OK** button to modify QoS.

Delete QoS

Step 1. In the QoS window, find the QoS you want to change, and click **Delete** in the Configure column.

Step 2. In the Delete QoS window, click **OK** to delete the QoS or click Cancel to discard the change.



Authentication

By configuring the Authentication, you can control the user's (Internal user or remote user who connect by VPN and IPSec) connection authority. The user has to pass the authentication to access to Internet.

Add New User

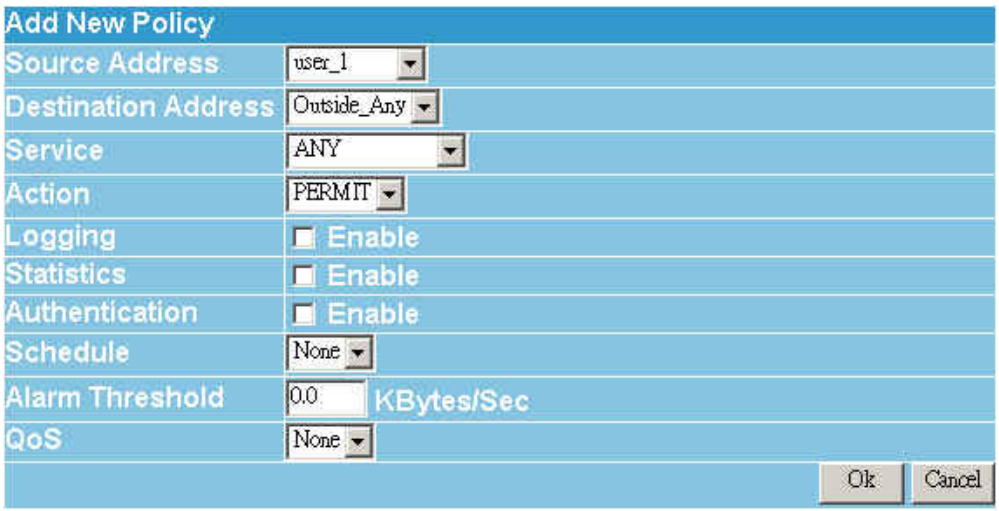
STEP 1．Setting the user's Address in **LAN** of **Address** function.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
user_1	192.168.1.2/255.255.255.255	00:0C:76:B4:E3:88	Modify Remove

STEP 2．Enter the following setting in **Authentication** function:

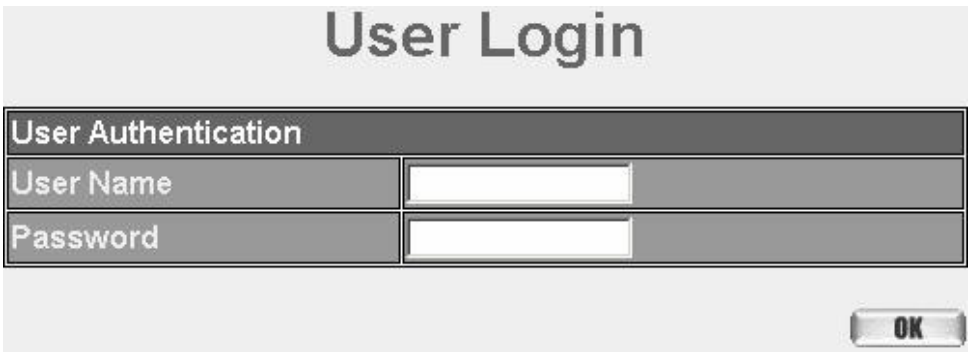
- Click **New User**
- **Auth-User Name:** Enter guest
- **Password:** Enter 1234
- **Confirm Password:** Enter 1234
- Click **OK**
- Complete Authentication Setting
-

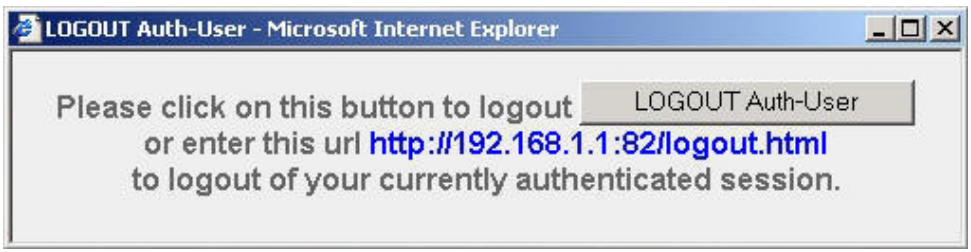
STEP 3．Add a policy in **Outgoing Policy** and input the Address and Authentication of STEP1, 2



STEP 4．When user_1 is going to access to Internet through browser, the authentication UI will appear in Browser. After entering the correct user name and password, click **OK** to access to Internet.

STEP 5．If the user does not need to access to Internet anymore and is going to logout, he/she can click **LOGOUT Auth-User** to logout the system. Or enter the Logout Authentication WebUI (http:// LAN Interface: Authentication port number/ logout.html) to logout.




LOGOUT Auth-User - Microsoft Internet Explorer
Please click on this button to logout
LOGOUT Auth-User
or enter this url http://192.168.1.1:82/logout.html
to logout of your currently authenticated session.

Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Security Bandwidth Manager.

What is Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:
(1). Outgoing: a client is in the LAN networks, while a server is in the WAN networks.
(2) Incoming, a client is in the WAN networks, while a server is in the LAN networks.

How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.
If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN network.

Entering the Outgoing window

Step 1. Click **Policy** on the left hand side menu bar,

Step 2. Click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.

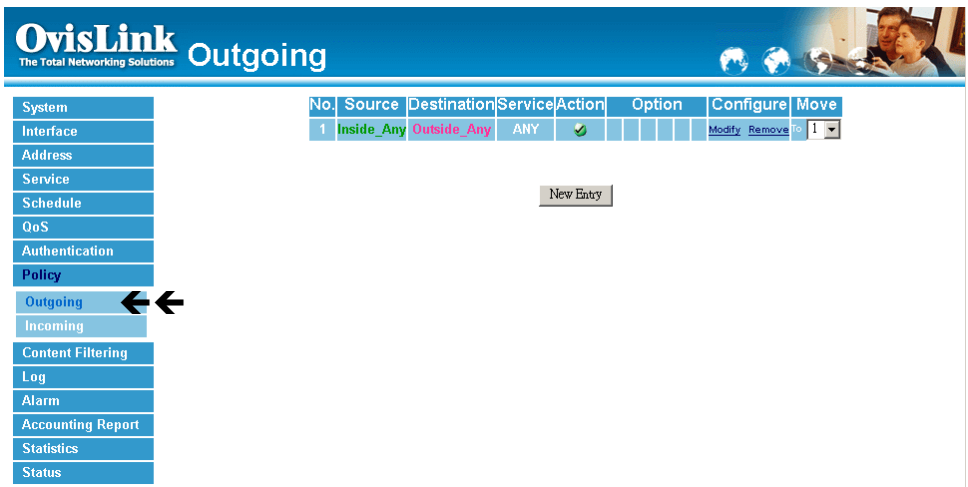


Figure7-1 Create an Outgoing Policy

The fields in the Outgoing window are:

- **Source**: source network addresses that are specified in the LAN section of Address menu, or all the LAN network addresses.
- **Destination**: destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- **Service**: specify services provided by WAN network servers.
- **Action**: control actions to permit or reject/deny packets from LAN networks to WANnetwork travelling through the Security Bandwidth Manager.
- **Option**: specify the monitoring functions on packets from LAN networks to WANnetworks travelling through the Security Bandwidth Manager.
- **Configure**: modify settings.
- **Move**: this sets the priority of the policies, number 1 being the highest priority.

Descriptions for **Policy** figures:

Figure	Name	Description
	Permit	Permit the specified packets from LAN network to WAN network.
	Block	Block the specified packets from LAN network to WAN network.
	Log	Traffic and event log function is enabled.
	Statistics	Flow statistics function is enabled.
	Schedule	The automatic execution function in Schedule table has been enabled.
	Alarm Threshold	Traffic and event alarm function is enabled.
	QoS	QoS function is enabled.

Remarks:

To view the traffic and event log of the system, click **Log** function in the menu bar on the left hand side.

To view the alarm records of the system, click **Alarm** function in the menu bar on the left hand side.

To view the statistics of the system, click **Statistics** function in the menu bar on the left hand side.

Security Bandwidth Manager can execute the schedule function automatically in a certain time and range. To modify the schedule, click the **Schedule** function in the menu baron the left hand side.

Security Bandwidth Manager can execute the QoS function function automatically. To modify the QoS, click the **QoS** function in the menu bar on the left hand side.

Adding a new Outgoing Policy

Click on the New Entry button and the Add New Policy window will appear.

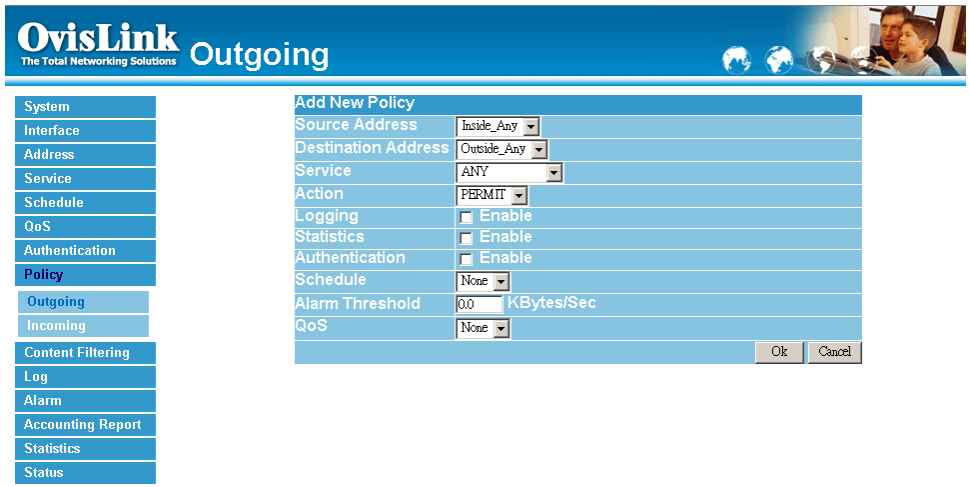


Figure7-2 Add a new Outgoing Policy

Source Address: Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

Destination Address: Select the name of the WANnetwork from the drop down list. The drop down list contains the names of all WANnetworks defined in the **WAN**section of the **Address** window. To create a new destination address, please go to the **WAN**section under the **Address** menu.

Service: Specified services provided by WANnetwork servers. These are srvices/application that are allowed to pass from the LAN network to the WANnetwork. Choose ANY for all services.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Schedule: Select the pre-defined schedule name from the pull-up menu. The policy will be executed in the specific time slot automatically.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

QoS: To determine if the QoS function can work in this Policy function.

Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

To change the Policy order of **Outgoing**, select the number from the pull-down menu on the right hand side **Move** column

Modifying an Outgoing policy

Step 1. In the **Modify Policy** window, fill in new settings.

Note: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→[Pre-defined],[Custom] or Group under **Service**).

Click **OK** to do confirm modification or click **Cancel** to cancel it.

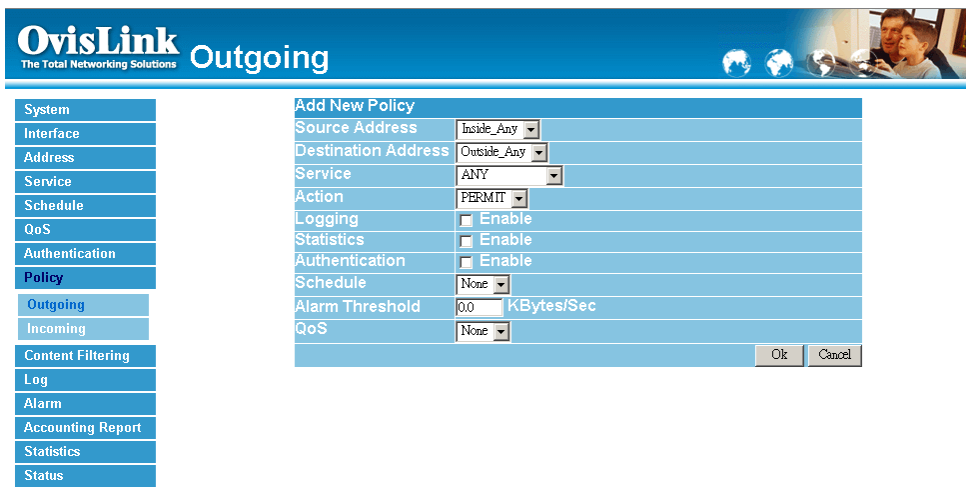


Figure7-3 Modify the Outgoing Policy

Source Address: Select the name of LAN from the pull-down menu.
The names of LAN listed in this pull-down menu are: the Source Addresses that are already set.
Destination Address: Select the name of WAN from the pull-down menu.
The names of WAN listed in this pull-down menu are: the Destination Addresses that are already set IP address of WAN network.

Service: Select the service item from the pull-down menu
Action: Select Permit or Block to allow or reject the specified packets from LAN network to WAN network.
Logging: Select **Enable** to enable the Logging function.
Statistics: Select **Enable** to enable the Statistics function.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

QoS: To determine if the QoS function can work in this Policy function.

Click **OK** to execute the new setting or click **Cancel** to discard changes.

If you want to change or add new items in the pull-down menu, go to the corresponding chapter for setup.

Source Address: **LAN** of **Address** menu

Destination Address: **WAN** of **Address** menu

Removing the Outgoing Policy

Step 1. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.

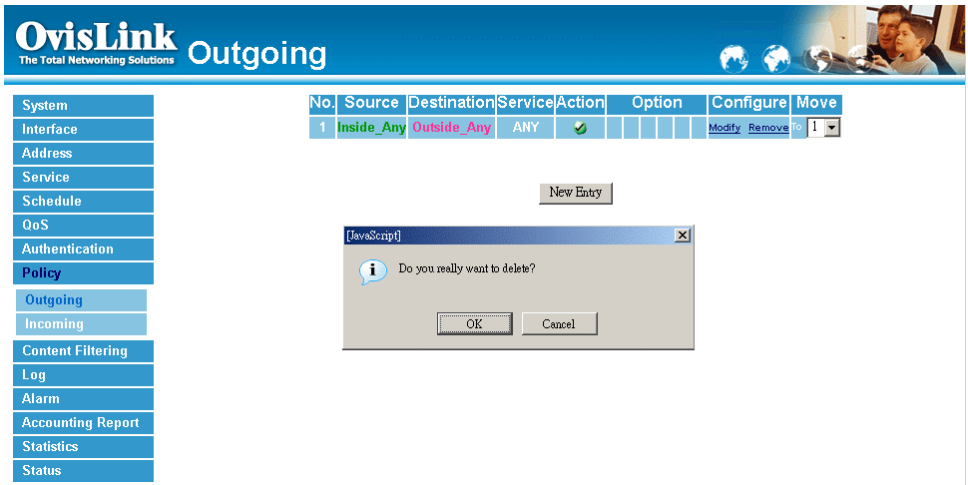


Figure7-4 Remove a Outgoing Policy

Incoming

This chapter describes steps to create policies for packets and services from the WAN network to the LAN network including Mapped IP and Virtual Server.

Enter Incoming window

Step 1. Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the WAN network to assigned Mapped IP or Virtual Server.

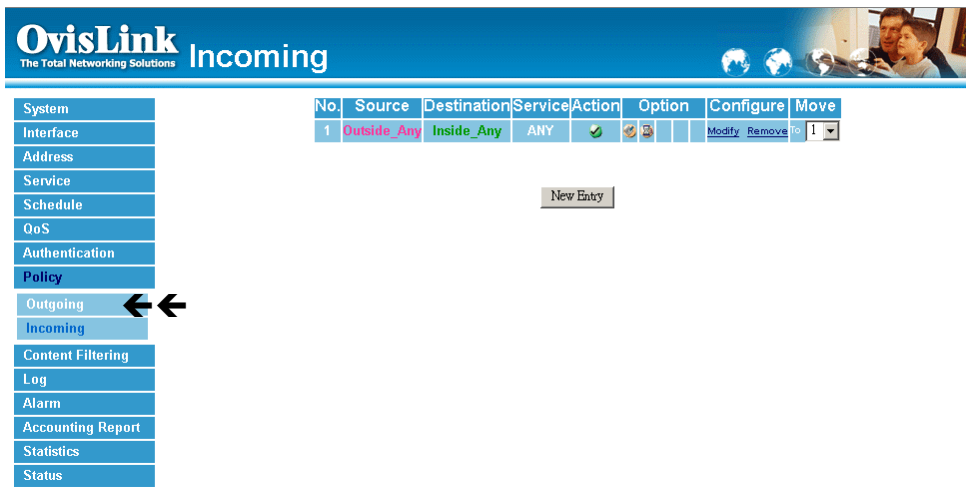


Figure7-5 Incoming Policy

Definition (Incoming):

No.: The numbering of the selected Policy, starting with Number 1.

Source Address: The WAN address was selected in WAN function of the Address Table.

Destination Address: The mapped IP or Virtual Server IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function.

Service: The service item provided by **Virtual Server** (or **Mapped IP**).

Action: Control actions to permit or reject packets from LAN networks to WAN network or Virtual Server (Mapped IP) traveling through the Security Bandwidth Manager.

Option: Control actions to monitor packets from WAN network or Virtual Server (Mapped IP) traveling through the Security Bandwidth Manager. The first column is the **logging** function. The second column is the **Statistics** function. The third column is the **Schedule** function. The

fourth column is the **Alarm Threshold** function. The fifth column is the **QoS** function. If the figures appear in the column, it means that the function is enabled. On the other hand, if there is no figures appeared in the column, it means that the function is not enabled.

The fields of the **Incoming** window are:

- **Source**: source networks which are specified in the WAN section of the Address menu, or all the WAN network addresses.
- **Destination**: destination networks, which are IP Mapping addresses or Virtual server network addresses created in Virtual Server menu.
- **Service**: services supported by Virtual Servers (or Mapped IP).
- **Action**: control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.
- **Option**: specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Security Bandwidth Manager.
- **Configure**: modify settings or remove incoming policy.
- **Move**: this sets the priority of the policies, number 1 being the highest priority.

Descriptions for **Policy** figures:

Figure	Name	Description
	Permit	Permit the specified packets from WAN to LAN.
	Block	Block the specified packets from WAN network to LAN network.
	Log	Traffic and event log function is enabled.
	Statistics	Flow statistics function is enabled.
	Schedule	The automatic execution function in Schedule table has been enabled.
	Alarm Threshold	Traffic and event alarm function is enabled.
	QoS	QoS function is enabled.

Remarks:

To view the traffic and event log of the system, click **Log** function in the menu bar on the left hand side.

To view the alarm records of the system, click **Alarm** function in the menu bar on the left hand side.

To view the statistics of the system, click **Statistics** function in the menu bar on the left hand side.

Security Bandwidth Manager can execute the schedule in time slot automatically. To modify the schedule, click the **Schedule** function in the menu bar.

Adding an Incoming Policy

Under **Incoming** of the **Policy** menu, click the New Entry button.

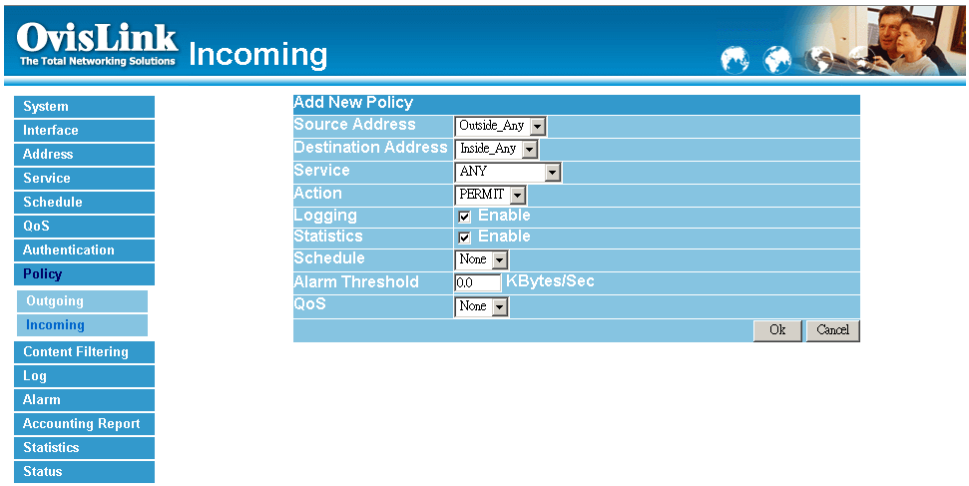


Figure7-6 Add a Incoming Policy

Source Address：Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are：the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Source Address：Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are：the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Destination Address：Select the name of LAN from the pull-down menu.

The names of LAN listed in this pull-down menu are：The Mapped IP or Server Virtual IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function. To add new items into the pull-down menu, go to Virtual Server window to configure.

Service：Select the service item from the pull-down menu.

Action：Select from the pull-down menu to determine the WAN, Virtual Server(or Mapped IP) packets are permitted or forbidden to pass. Select Permit or Forbid.

Logging：Select Enable to enable the Logging function.

Statistics：Select Enable the enable the Statistics function.

Schedule：Select the item listed in the schedule to enable the policy to automatically execute

the function in a certain time and range.

Alarm Threshold：To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

QoS：To determine if the QoS function can work in this Policy function.

Click **OK** to execute the new setting or click Cancel to discard changes.

To change the Policy order of Incoming, select the number from the pull-down menu on the right hand side **Move** column

Modifying Incoming Policy

Step 1. In the Modify Policy window, fill in new settings.

Step 2. Click **OK** to save modifications or click **Cancel** to cancel modifications.

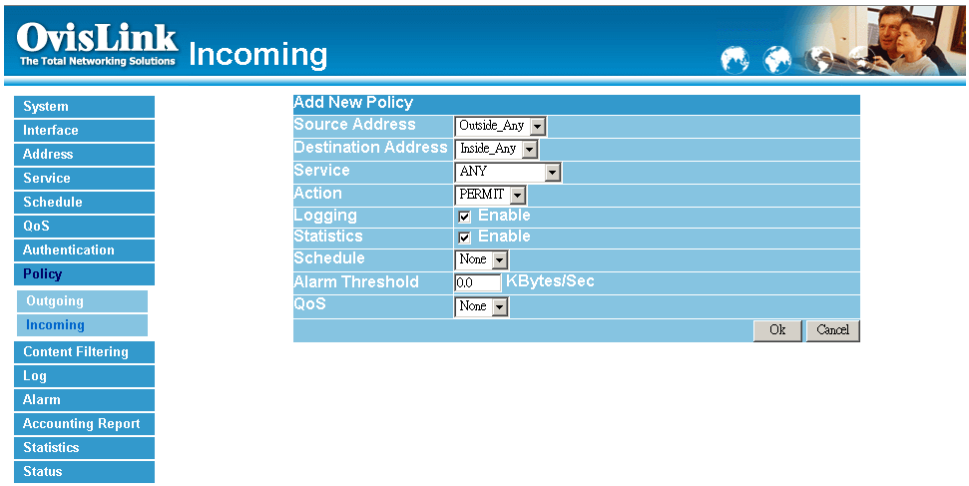


Figure7-7 Modify an Incoming Policy

Source Address：Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are：the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Destination Address：Select the name of LAN from the pull-down menu.

The names of LAN listed in this pull-down menu are：The Mapped IP or Server Virtual IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function. To add new items into the pull-down menu, go to Virtual Server window to configure.

Service：Select the service item from the pull-down menu.

Action：Select from the pull-down menu to determine the WAN, Virtual Server(or Mapped IP) packets are permitted or forbidden to pass. Select Permit or Forbid.

Logging：Select Enable to enable the Logging function.

Statistics：Select Enable the enable the Statistics function.

Schedule：Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold：To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

QoS：To determine if the QoS function can work in this Policy function.

Click **OK** to execute the new setting or click Cancel to discard changes.

*if you want to change or add new items into the pull-down menu, go to the original configuration unit***.**

Removing an Incoming Policy

Step 1. In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.

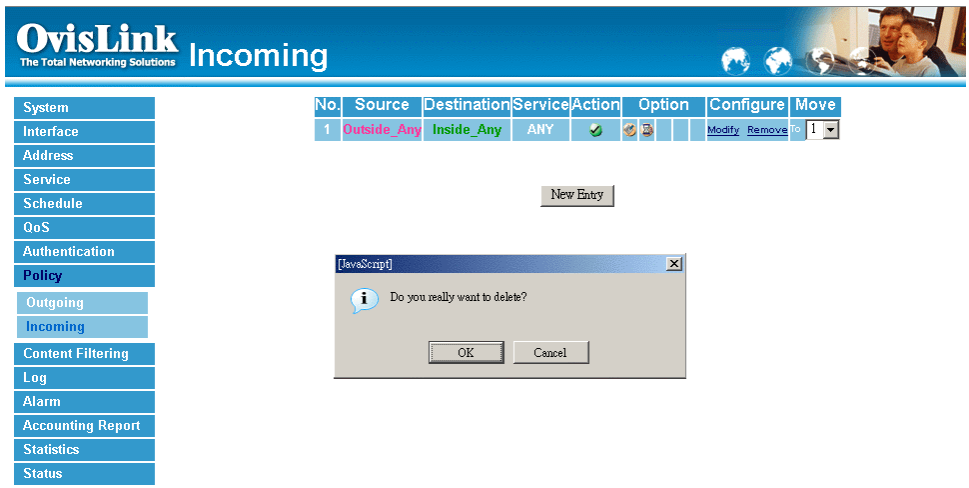


Figure7-8 Remove an Incoming Policy

Content filtering

Content Filtering includes “**URL Blocking**” and “**General Blocking**”

URL Blocking：The administrator can use a complete domain name, key word, “～” or “＊” to make rules for specific websites.

General Blocking：To let Popup、ActiveX、Java、Cookie in or keep them out.

Apply Policy

Administrator can use a complete domain name, key word, wild card（〝～〞or 〝＊〞）to permit or block access to certain websites.

URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from an LAN network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window

Step 1. Click on **URL Blocking** under the **Configuration** menu bar.

Step 2. Click on **New Entry.**

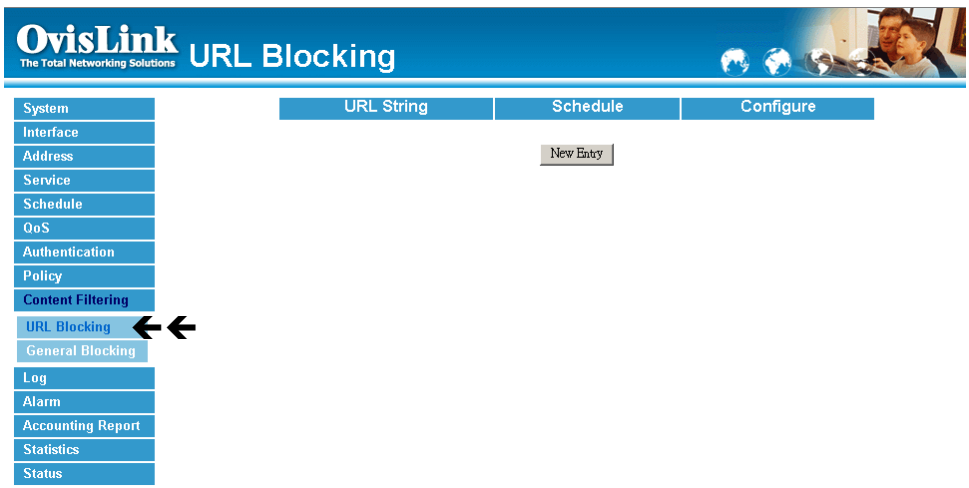


Figure8-1 Enter the URL Blocking

Definition:

Block String：The domain name that is permitted or blocked to enter by Security Bandwidth Manager.

Schedule：This schedule is used to set the time of permitting or blocking certain websites to enter.

Configuration：To change the settings of URL Blocking, click **Modify** to change the parameters; click **Delete** to delete the settings.

How to use URL Blocking：

Description of signs：〝～〞 means to permit to enter；〝＊〞 means wild card。

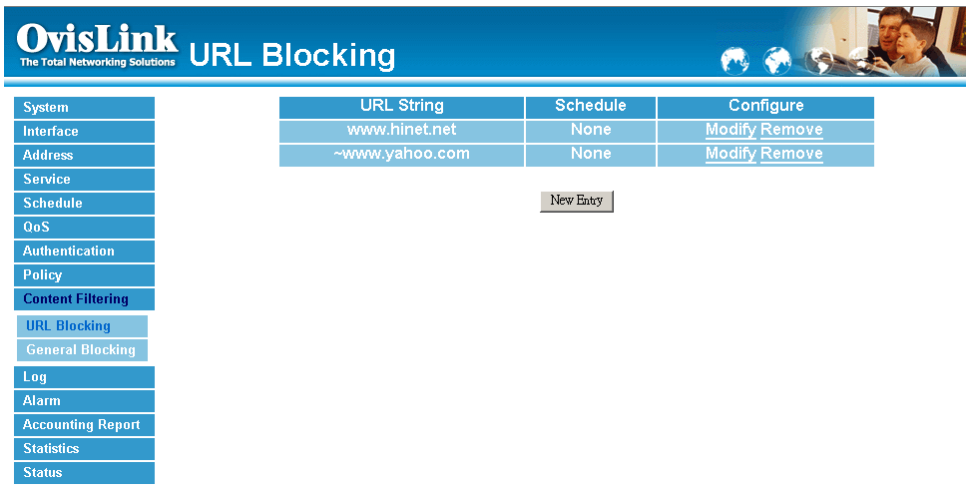
To block certain websites：Enter the complete domain name or key words of the website you want to block in the Block String column. For example, www.yahoo.com or yahoo。

Only permit certain websites to enter：

Enter the complete domain name or key words of the website you permit to enter and add the sign 〝～〞 in the front.（For example, ～www.yahoo.com or ～yahoo）。

After setting all the websites you permit entering, add the sign 〝＊〞 in front of the last website you want to permit entering. Note：This instruction is always put in front of the last one.

If you want to add new websites to permit entering, you have to remove the instruction of blocking all websites and then key in the new domain name, after that, add the block all instruction.



Adding a URL Blocking policy

Step 1. After clicking **New Entry**, the **Add New Block String** window will appear.

Step 2. Enter the URL of the website to be blocked.

Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.

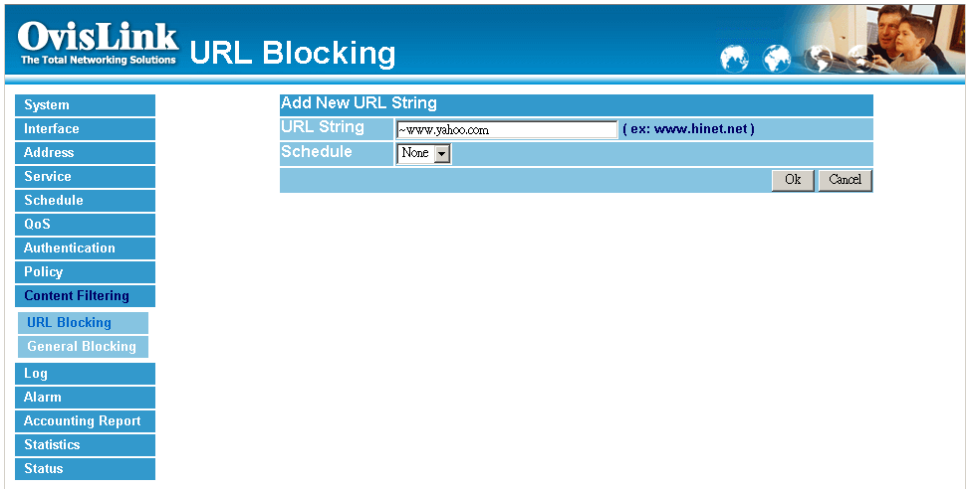


Figure8-2 Add a New URL Blocking

Modifying a URL Blocking Policy

Step 1. In the **URL Blocking** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2. Make the necessary changes needed.

Step 3. Click on **OK** to save changes or click on **Cancel** to discard changes.

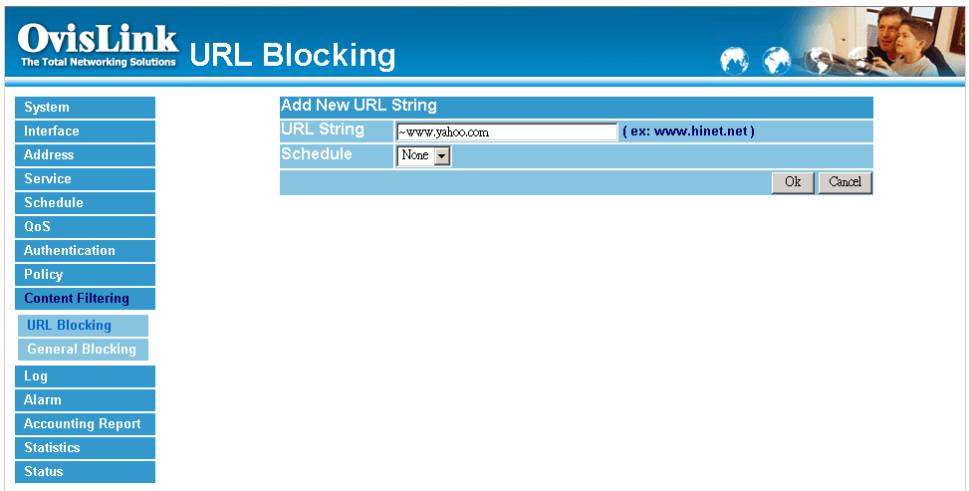


Figure8-3 Modify the URL Blocking

Removing a URL Blocking policy

Step 1. In the **URL Blocking** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the policy or click on **Cancel** to discard changes.

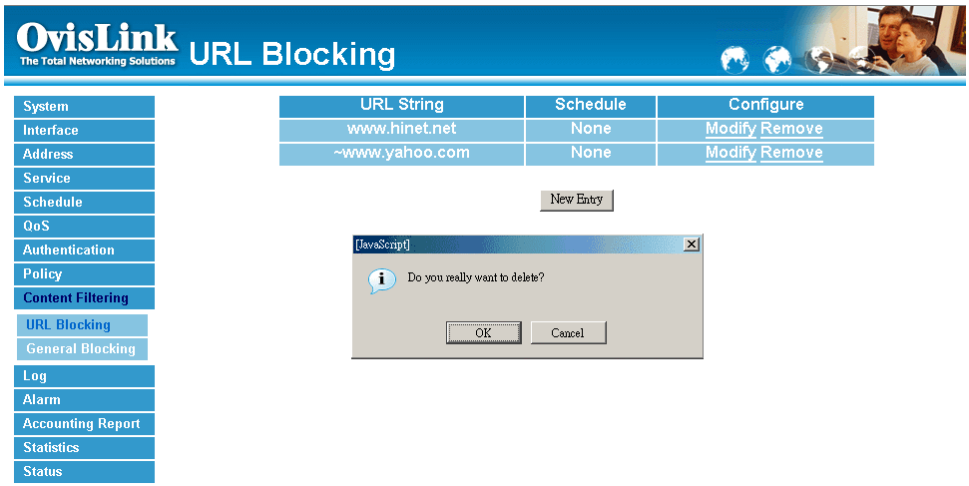
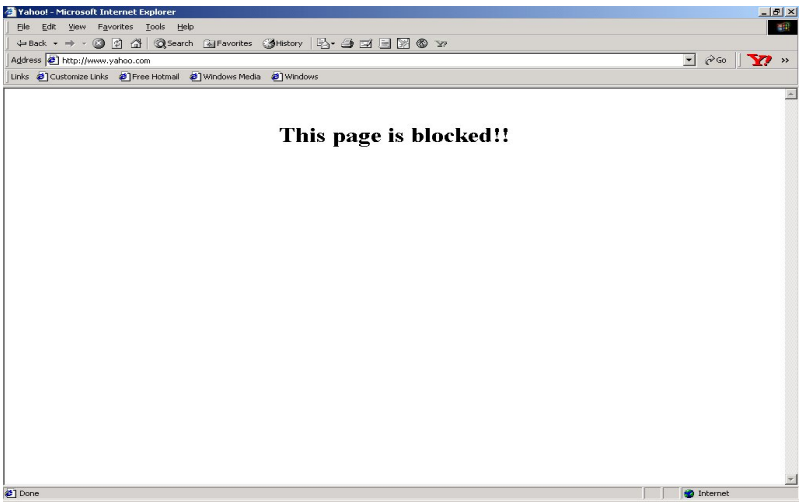


Figure8-4 Remove a URL Blocking

Blocked URL site:

When a user from the LAN network tries to access a blocked URL, the error below will appear.



General Blocking

To let Popups, ActiveX, Java, or Cookies in or keep them out.

Step 1: Click **Content Filtering** in the menu.

Step 2: **General Blocking** detective functions.

Popup filtering: Prevent pop-up boxes from appearing.

ActiveX filtering: Prevent ActiveX packets.

Java filtering: Prevent Java packets.

Cookie filtering: Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.

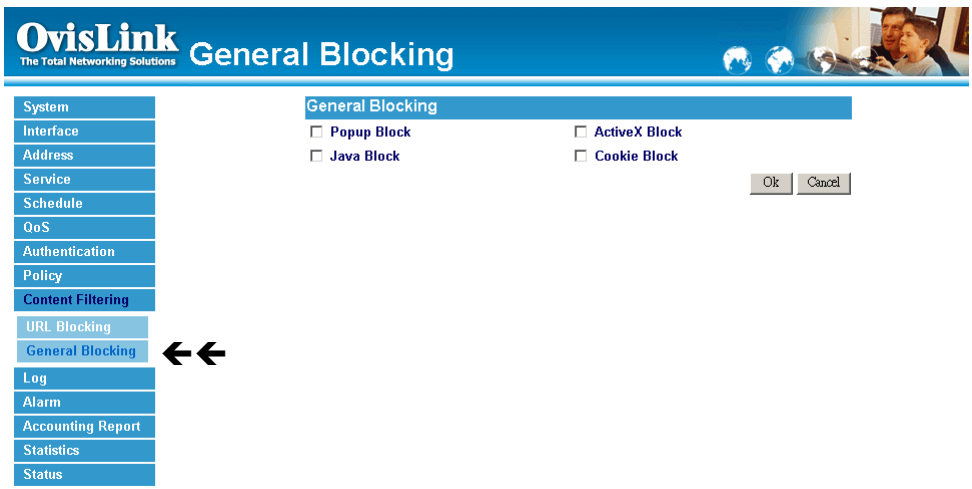


Figure8-5 General Blocking Policy

When the system detects the setting, the Security Bandwidth Manager will spontaneously work.

Virtual Server

The Security Bandwidth Manager separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through Security Bandwidth Manager's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

The Security Bandwidth Manager's Virtual Server can solve this problem. A virtual server has set the real IP address of the Security Bandwidth Manager's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Security Bandwidth Manager translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which is opposite to NAT), but there are still some differences:

- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real WANIP address is mapped to one private LAN IP address.

Entering the Mapped IP window

Step 1. Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.

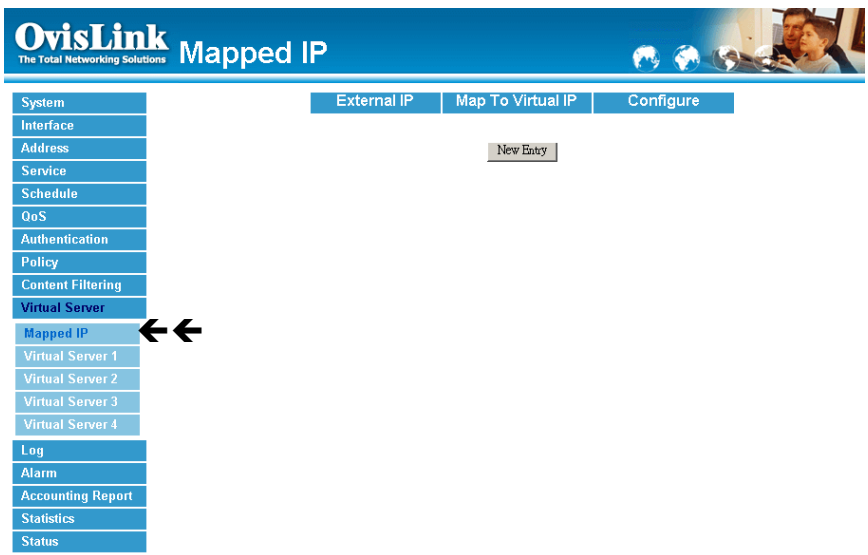


Figure9-1 Mapped IP

Definition:

External IP：WAN IP Address.

Map to Virtual IP：The IP address which WAN maps to the virtual network in the server.

Configure：To change the setting, click Configure to modify the parameters; click delete to delete the setting.

Adding a new IP Mapping

Step 1. In the **Mapped IP** window, click the New Entry button. The Add New Mapped IP window will appear.

- **WAN IP**: select the WAN public IP address to be mapped.
- **Internal IP**: enter the LAN private IP address will be mapped 1-to-1 to the WAN IP address.

Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.

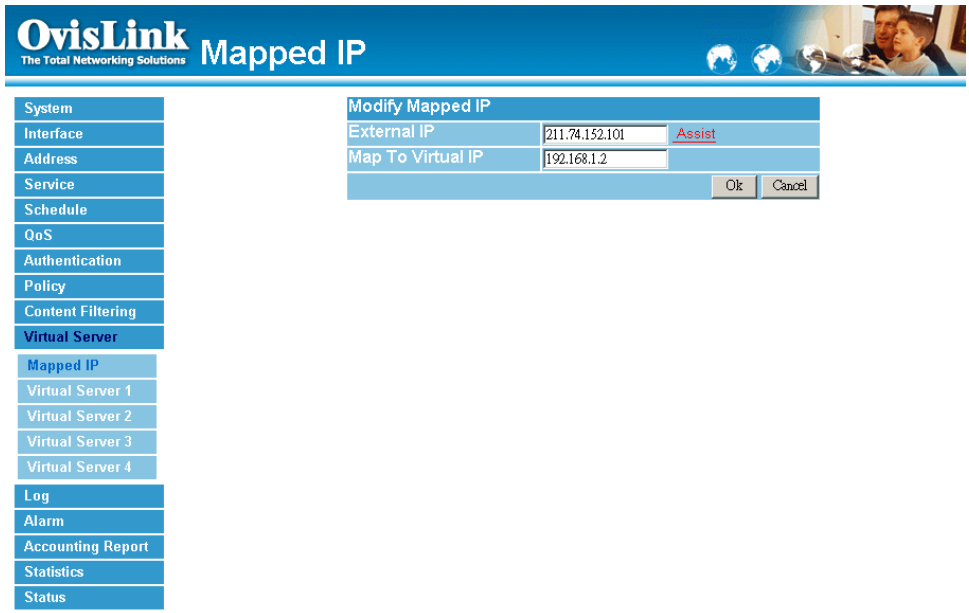


Figure9-2 Add New Mapped IP

Modifying a Mapped IP

Step 1. In the **Mapped IP** table, locate the Mapped IP you want it to be modified and click its corresponding Modify option in the Configure field.

Step 2. Enter settings in the Modify Mapped IP window.

Step 3. Click **OK** to save change or click **Cancel** to cancel.

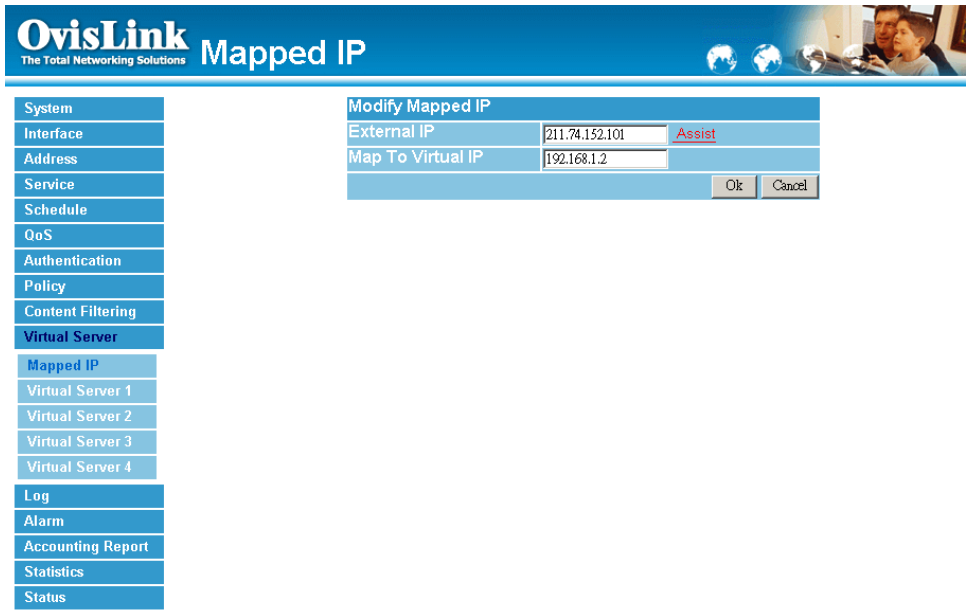


Figure9-3 Modify Mapped IP

Note: *A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.*

Removing a Mapped IP

Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up window, click **OK** to remove the Mapped IP or click **Cancel** to cancel.

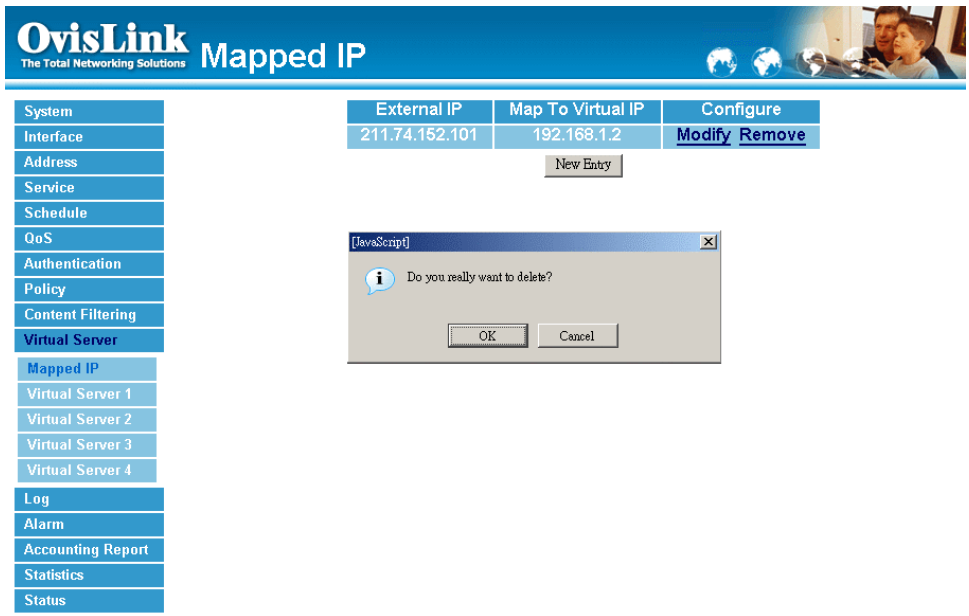


Figure9-4 Remove Mapped IP

Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds an WANIP to an LAN IP, virtual server binds WAN IP ports to LAN IP ports.

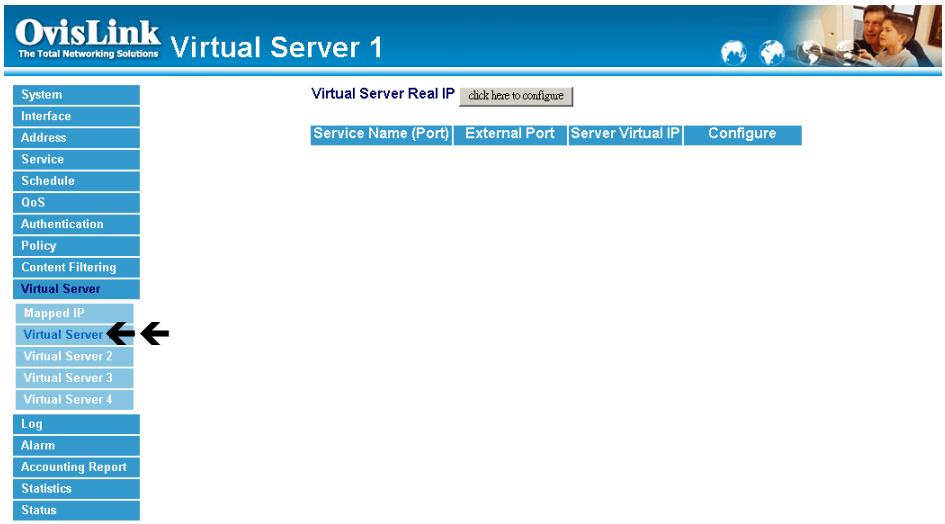


Figure9-5 Virtual Server

Definition:

Virtual Server IP：The WAN IP address configured by the virtual server. Click "**Click here to configure**" button to add new virtual server address.

Service name：The service names that provided by the virtual server.

Port：The TCP/UDP ports that present the service items provided by the virtual server.

Server Virtual IP：The virtual IP which mapped by the virtual server.

Configure：To change the service configuration, click **Configure** to change the parameters; click **Delete** to delete the configuration.

This virtual server provides four real IP addresses, which means you can setup four virtual servers at most （Setup under the Virtual Server sub-selections Virtual Server 1/2/3/4 in the menu bar on the left hand side.） The administrator can select Virtual Server1/2/3/4under Virtual Server selection in the menu bar on the left hand side, click **Server Virtual IP** to add or change the virtual server IP address; click **"Click here to configure"** to add or change the virtual server service configuration.

Adding a Virtual Server

Step 1. Click an available virtual server from **Virtual Server** in the **Virtual Server** menu bar to enter the virtual server configuration window. In the following, Virtual Server is assumed to be the chosen option:

Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the WAN network.

Step 3. Select an IP address from the drop-down list of available WAN network IP addresses.

Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.

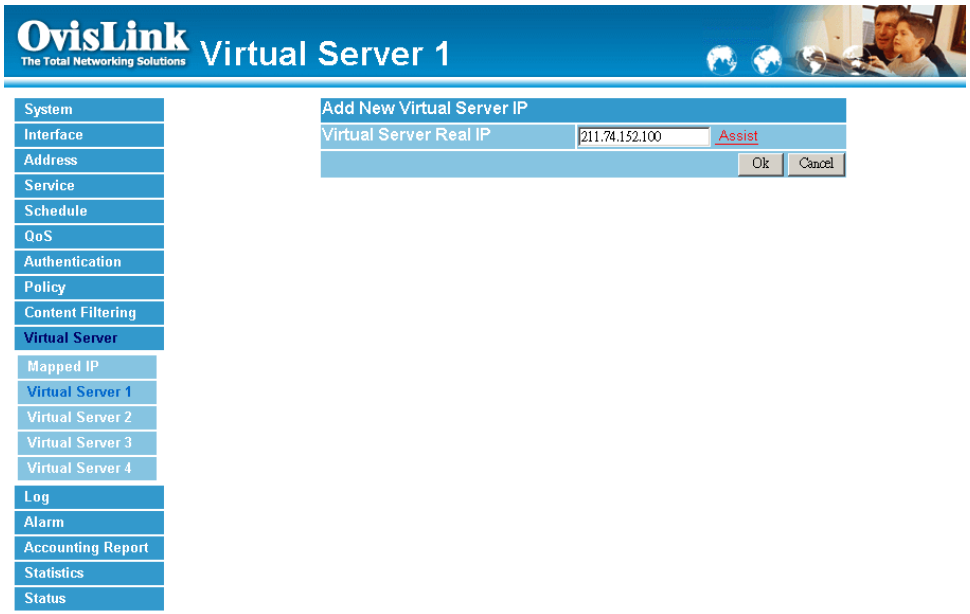


Figure 9-6 Add New Virtual Server

Modifying a Virtual Server IP Address

Step 1. Click the virtual server to be modified Virtual Server under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.

Step 2. Click on the Virtual Server's IP Address button at the top of the screen.

Step 3. Choose a new IP address from the drop-down list.

Step 4. Click **OK** to save new IP address or click **Cancel** to discard changes.

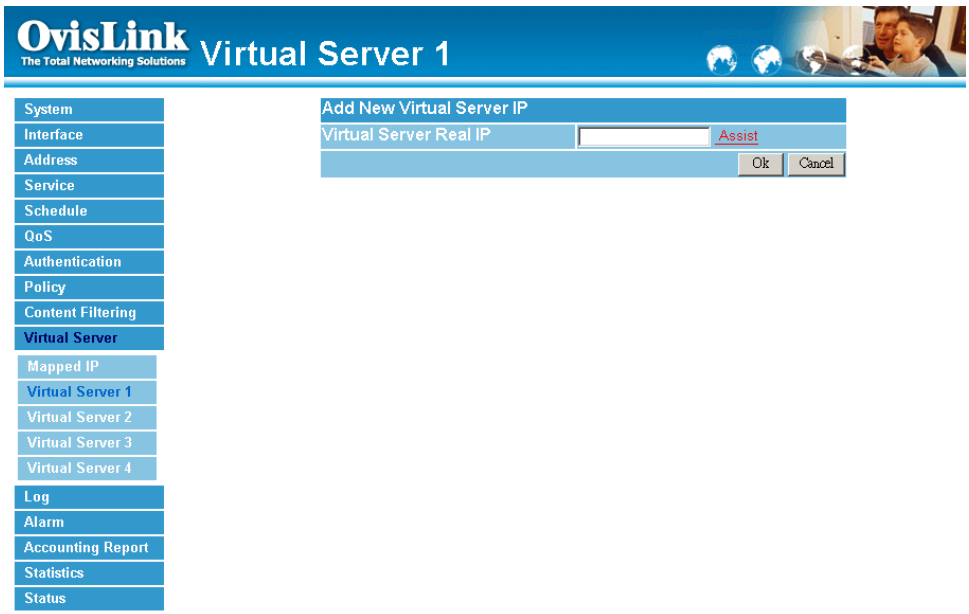


Figure9-7 Modify Virtual Server IP Address

Removing a Virtual Server

Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.

Step 2. Click the Virtual Server's IP Address button at the top of the screen.

Step 3. Select Disable in the drop-down list in.

Step 4. Click **OK** to remove the virtual server.

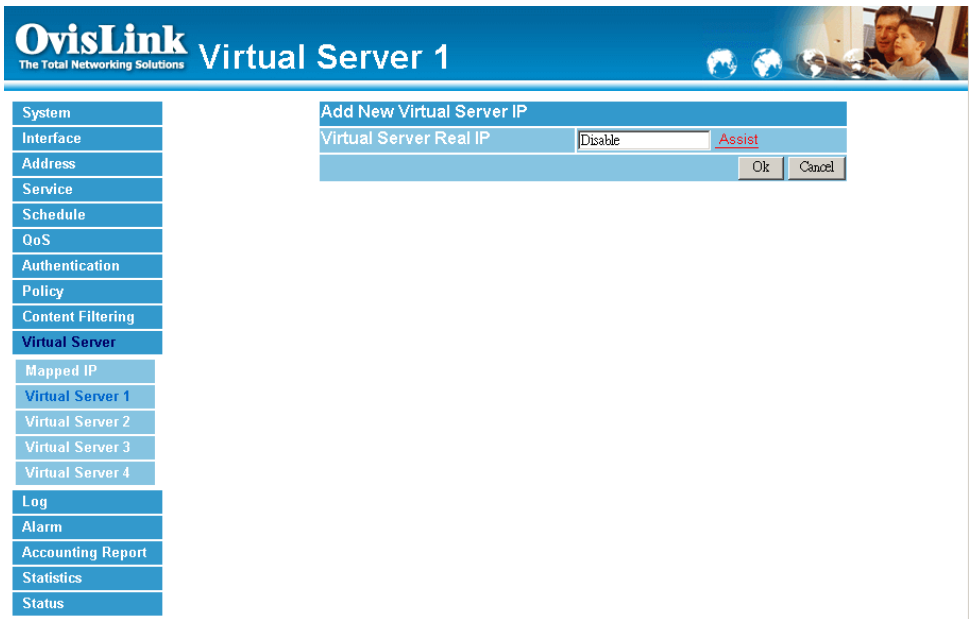


Figure9-8 Remove Virtual Server

Setting the Virtual Server's services

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

Step 2. In the Virtual Server Configurations window:

- **Server Virtual IP:** displays the WAN IP address assigned to the Virtual Server
- **External Service Port:** select the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Service:** select the service from the pull down list that will be provided by the Virtual Server.
- **Internal Server IP**：The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance.

Step 3. Enter the IP address of the LAN network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

Note: *The services in the drop-down list are all defined in the Pre-defined and Custom section of the* ***Service*** *menu.*

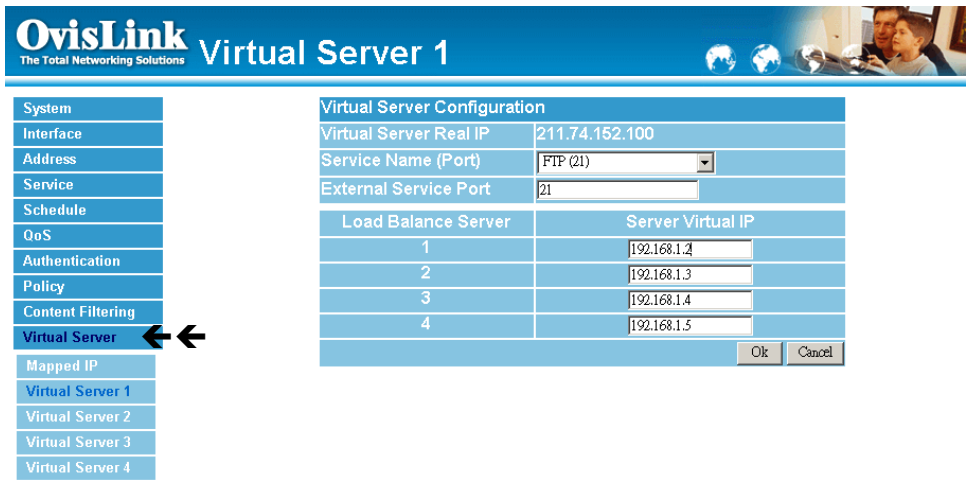


Figure9-9 Add New Virtual Server

Adding New Virtual Server Service Configuration

Step 1. Select Virtual Server in the menu bar on the left hand side, and then select Virtual Server 1/2/3/4 sub-selections.

Step 2. In Virtual Server 1/2/3/4 Window, click "**Click here to configure**" button.

Step 3. Enter the parameters in the Server Virtual IP column.

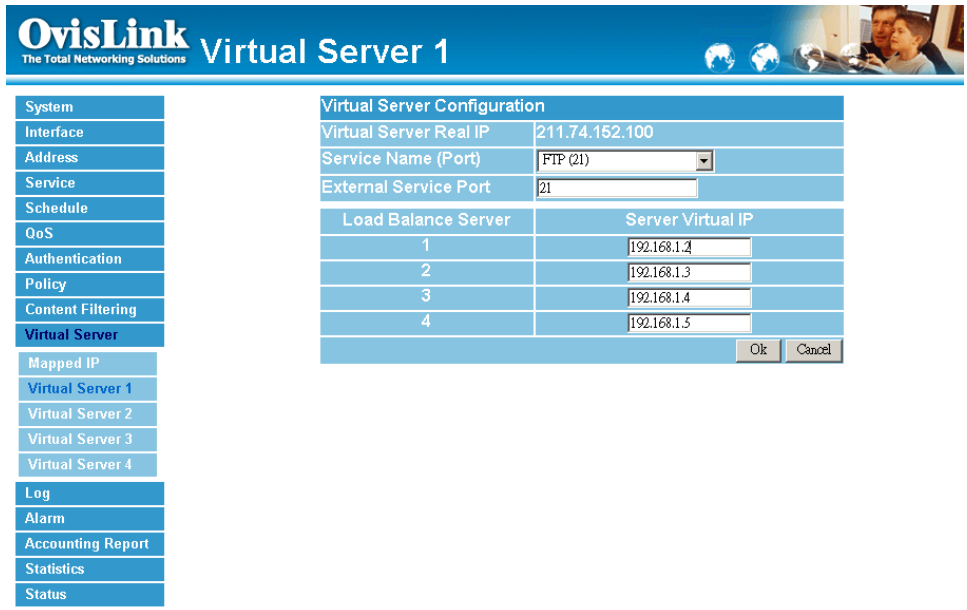


Figure9-10 Add Virtual Server

Server Virtual IP：Enter the WAN IP address configured by the virtual server.

Service Name (Port)：Click the pull-down menu the system will display you the service item port.

Service Name：The service names that provided by the virtual server.

Internal Server IP：The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance.

Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.

The administrator can click the "Click here to configure**" button in the Virtual Server window to add the service items of virtual server. Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.**

Modifying the Virtual Server configurations

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. In the Virtual Server Configuration window, enter the new settings.

Step 3. Click **OK** to save modifications or click **Cancel** to discard changes.

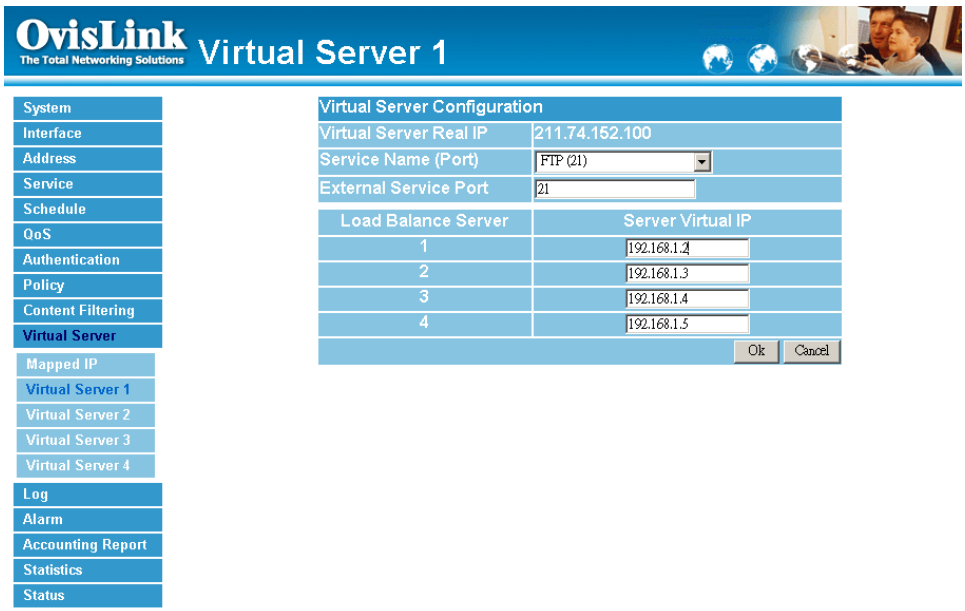


Figure9-11 Modify Virtual Server

WAN：Enter the WAN IP address that configured by the virtual server.

Port：Click the pull-down menu and the system will display you the service item port

Service Name：The service names provided by the virtual server.

Server Virtual IP：Enter the internal IP address mapped by the virtual server. Four computer IP addresses can be set at most.

Click **OK** to execute the change of the virtual server, or click **Cancel** to discard changes.

If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server, you have to remove this configuration of Policy, and then you can execute the modification or configuration.

Removing the Virtual Server service

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the service or click **Cancel** to cancel removing.

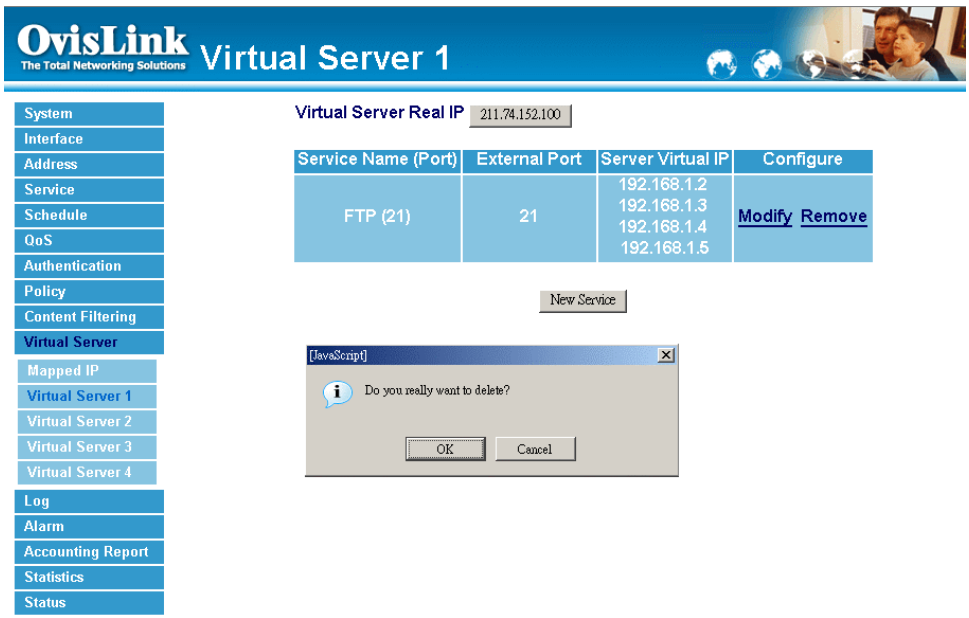


Figure9-12 Remove Virtual Server

If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server unless you have already removed this configuration of Policy.

Log

The Security Bandwidth Manager supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the Security Bandwidth Manager.

What is Log?

Log records all connections that pass through the Security Bandwidth Manager's control policies. Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.

How to use the Log

The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

Traffic Log

The Administrator queries the Security Bandwidth Manager for information, such as source address, destination address, start time, and Protocol port, of all connections.

Entering the Traffic Log window

Step 1. Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.

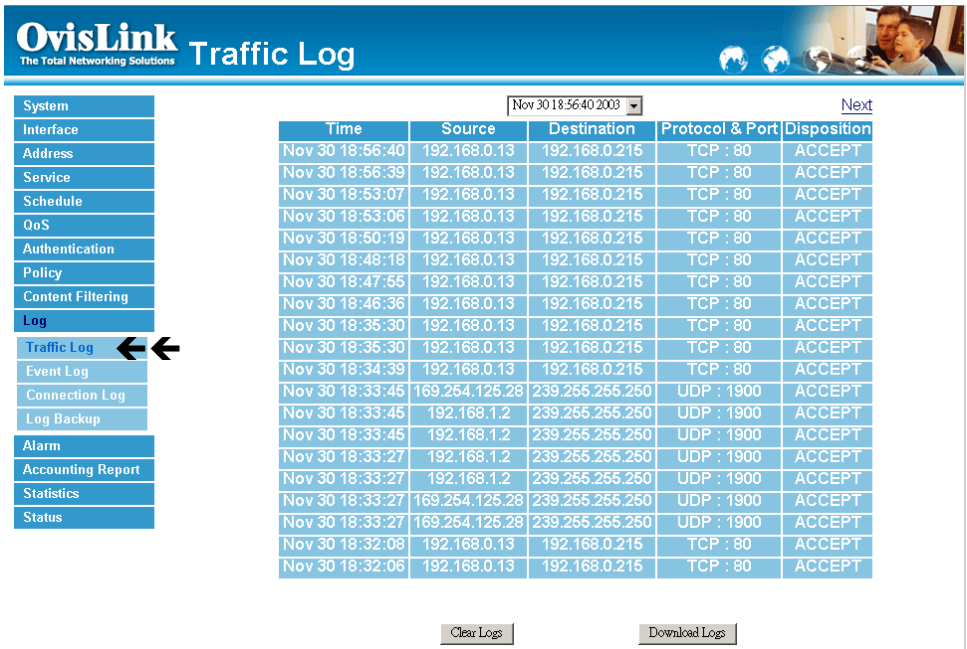


Figure10-1 Traffic Log

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

- **Time**: The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol & Port:** Protocol type and Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

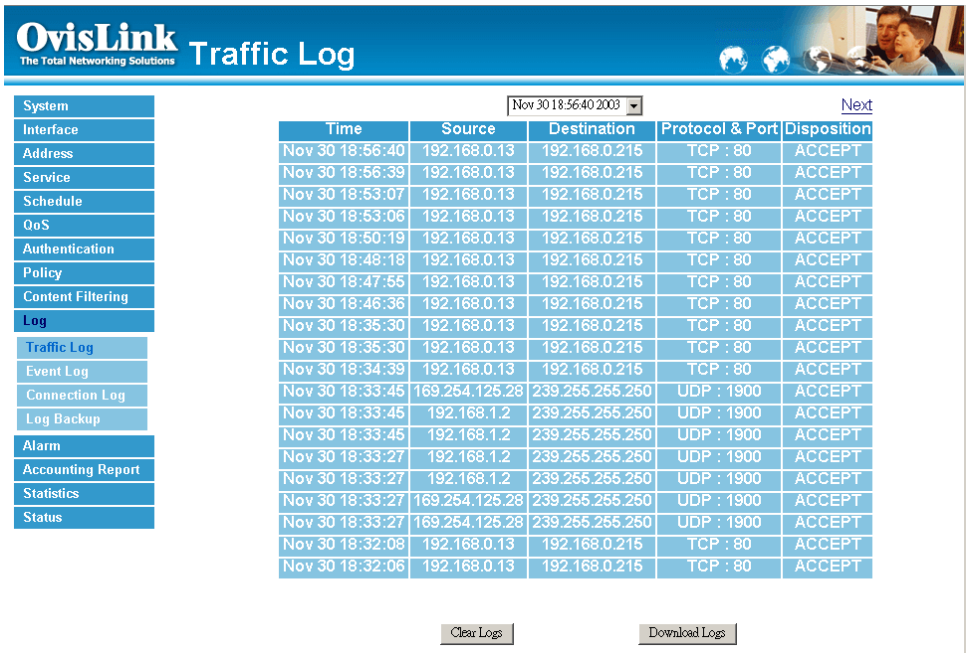


Figure10-2 Traffic Log

Clearing the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.

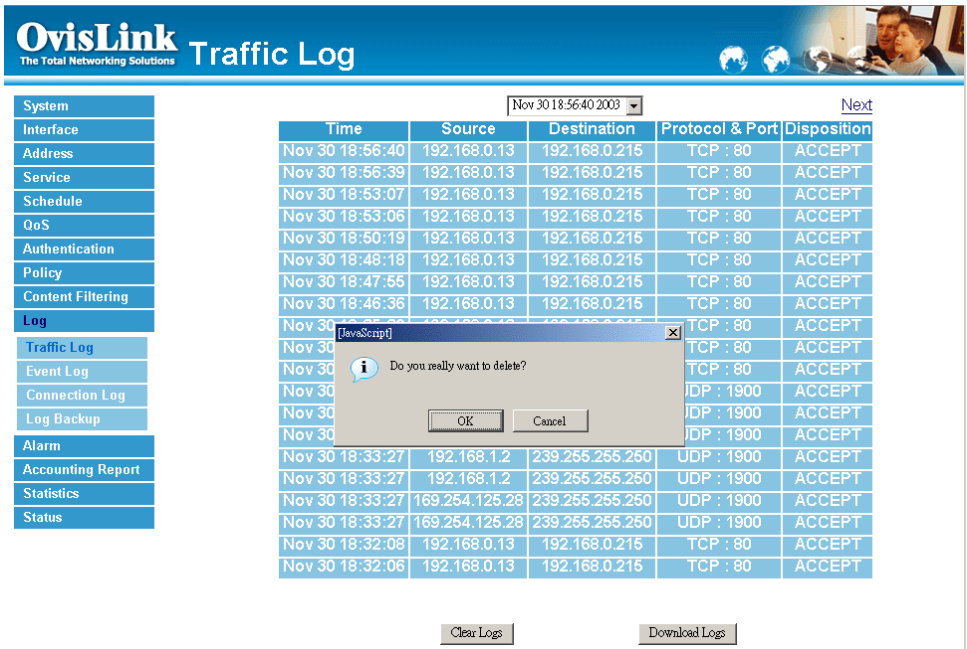


Figure10-3 Clear Traffic Logs

Event Log

When the Security Bandwidth Manager WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.

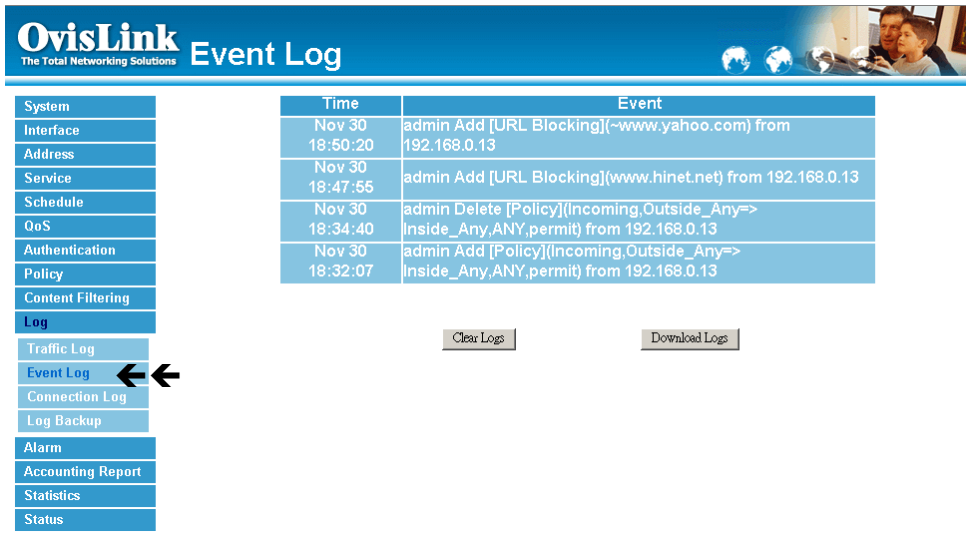


Figure10-4 Event Log

Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

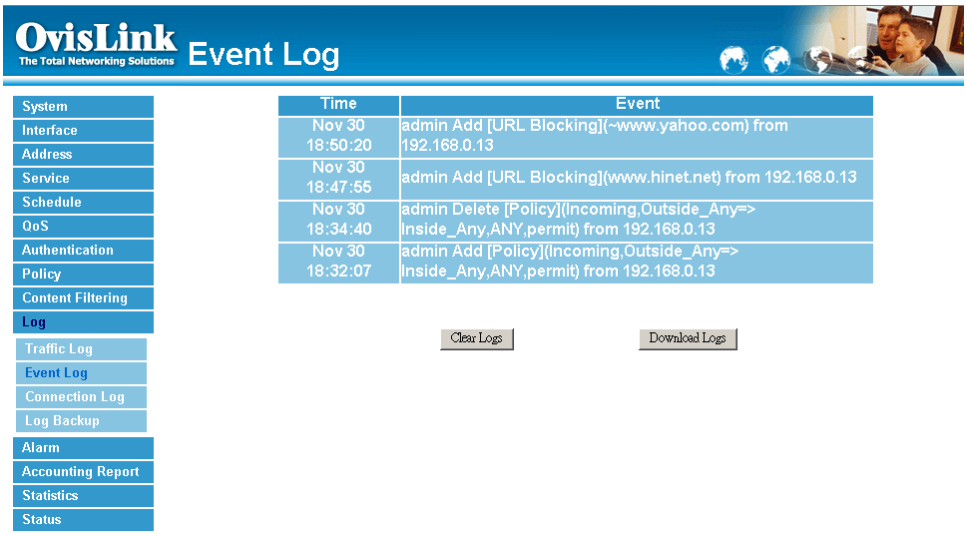


Figure10-5 Download the Event Logs

Clearing the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.

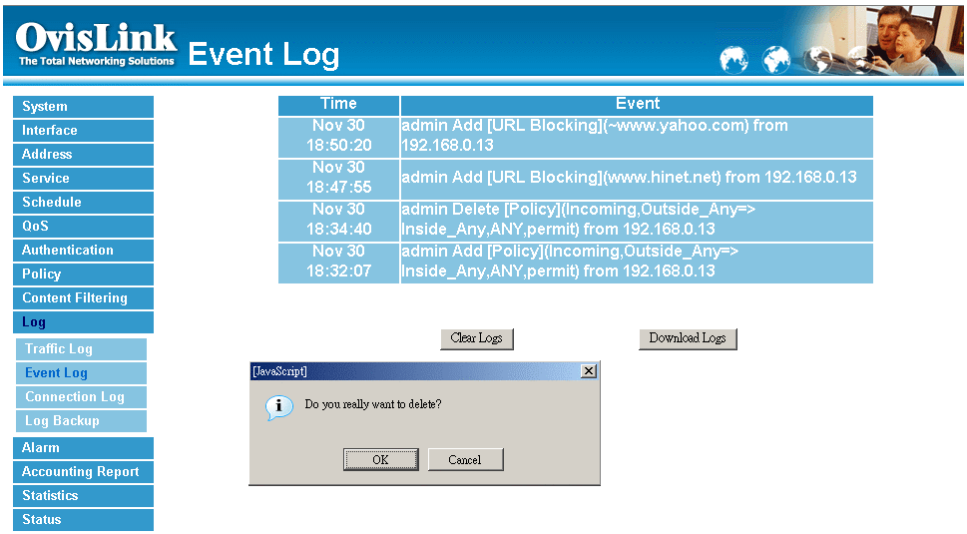


Figure10-6 Clear the Event Logs

Connection Log

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.

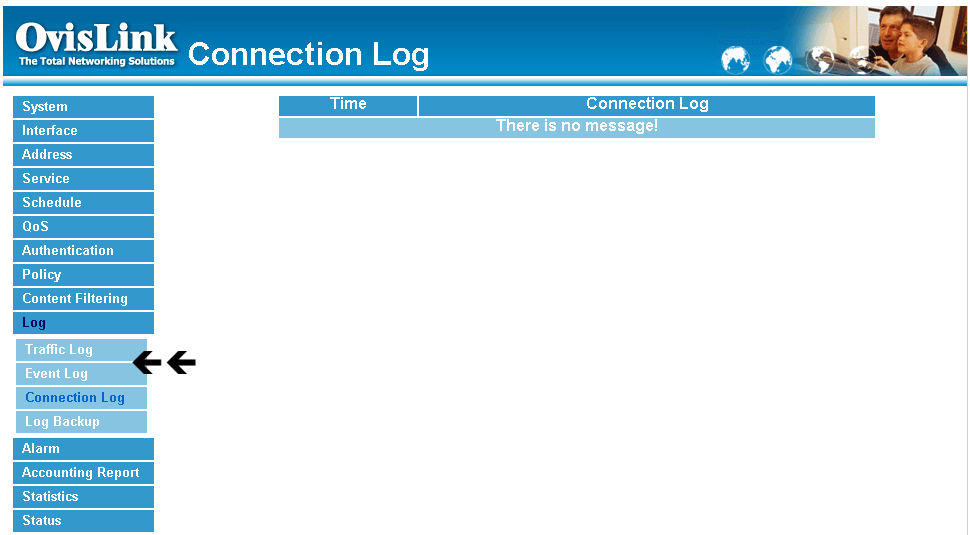


Figure10-7 Connection Log

Definition:

Time：The start and end time of connection.

Connection Log：Event description during connection.

Download Logs

Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.

Step 2. In Connection Log window, click the **Download Logs** button.

Step 3. In the Download Logs window, save the logs to the specified location.

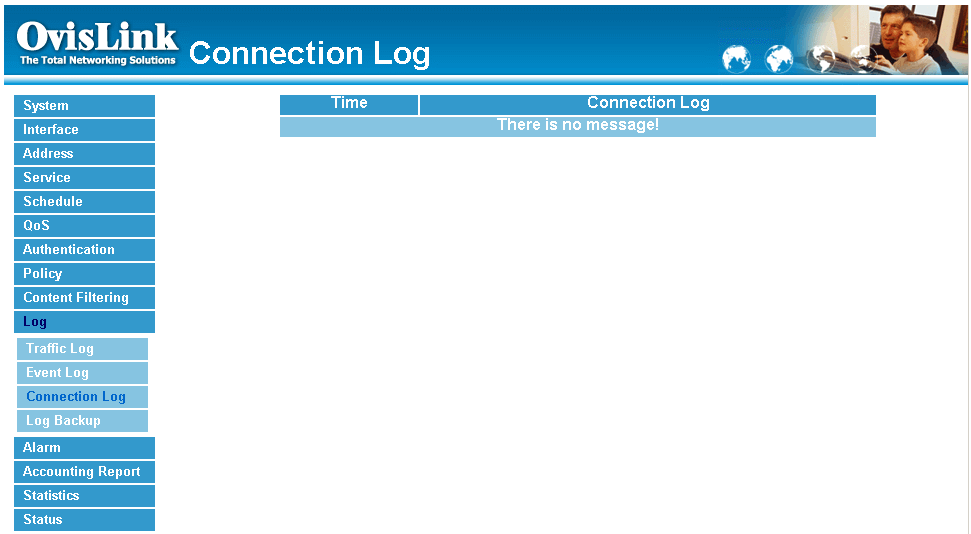


Figure10-8 Connection Log

Clear Logs

Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.

Step 2. In Connection Log window, click the **Clear Logs** button.

Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.

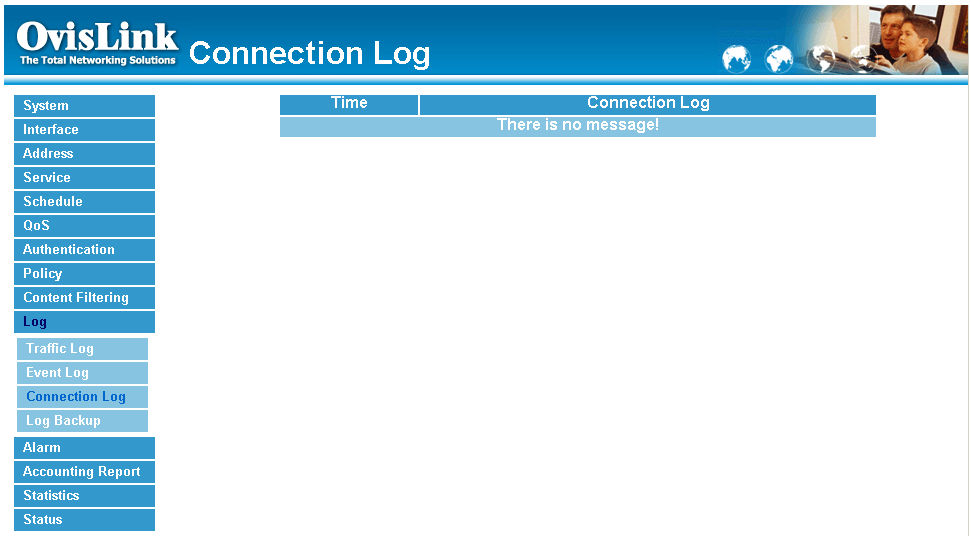


Figure10-9 Clear the Connection Logs

Log Backup

Step 1. Click **Log →Log Backup**.

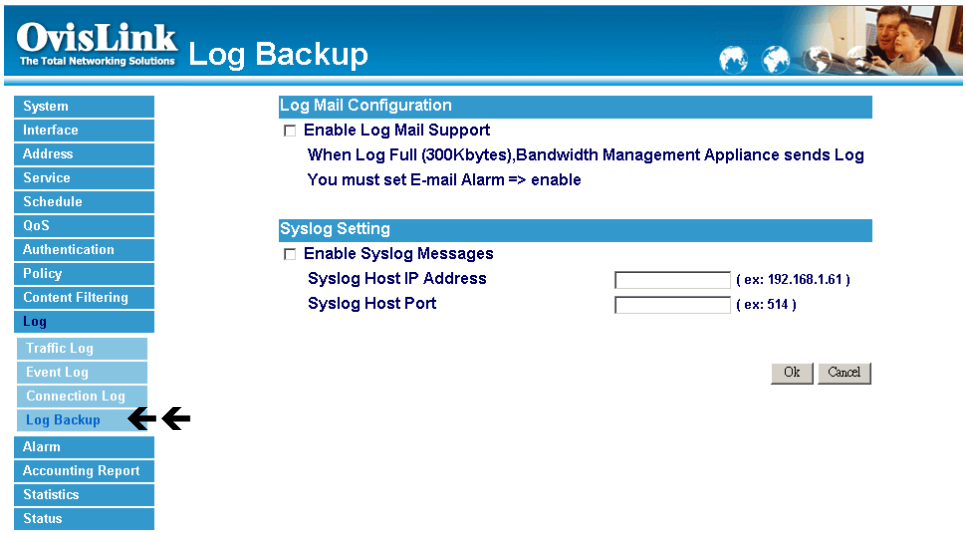


Figure10-10 Log Backup

Log Mail Configuration：When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.。

Note: Before enabling this function, you have to enable E-mail Alarm in Administrator.

Syslog Settings：If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

*To restart Connection Log, click the **Refresh** button on the right hand side in Log window.*

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.

Step 2. Go to **LOG →Log Backup.** Check to enable **Log Mail Support.** Click **OK.**

System Settings/Enable Syslog Message

Step 1. Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.

Step 2. Click **OK**.

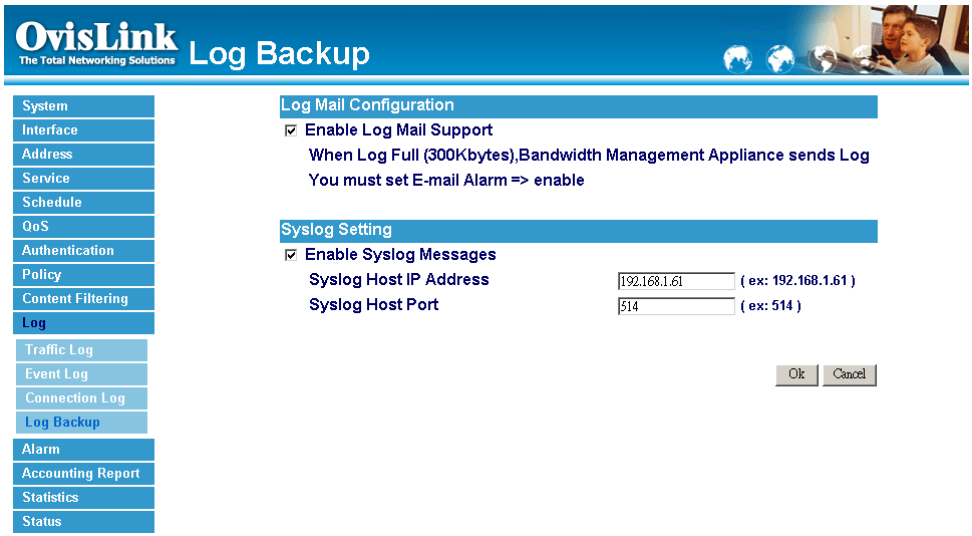


Figure10-11 Log Backup

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG →Log Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG →Log Backup**. Uncheck to disable Settings Message. Click **OK**.

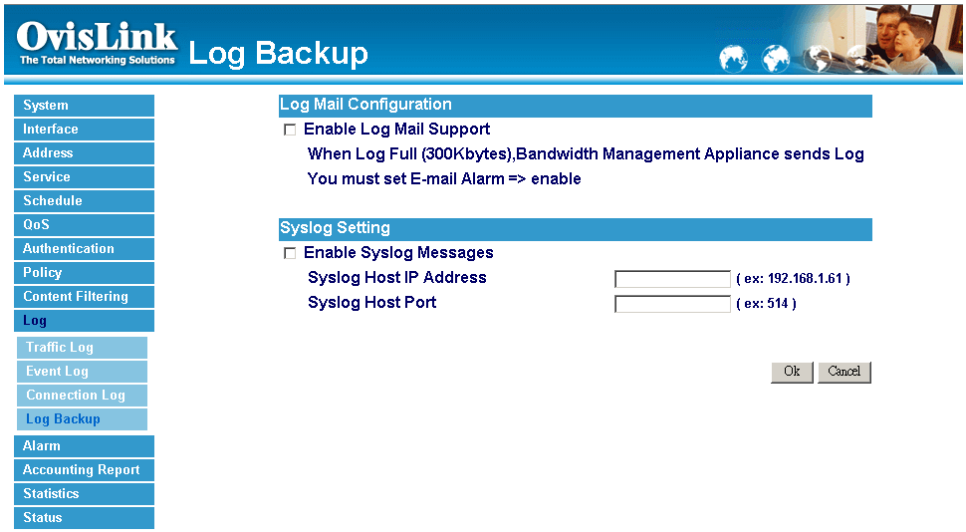


Figure10-12 Disable Log Backup

Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the Security Bandwidth Manager has logged.
Security Bandwidth Manager has two alarms: **Traffic Alarm** and **Event Alarm**.

Traffic alarm:

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Event alarm:

When Security Bandwidth Manager detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

How to apply Traffic Alarm

The administrator can use Traffic Alarm to track the Source Address, Destination Address, network service and the status of network. The administrator can save Traffic Logs and Event Logs for a pre-determined time and then delete them to keep the newest log.

Traffic Alarm

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Entering the Traffic Alarm window

Step 1. Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.

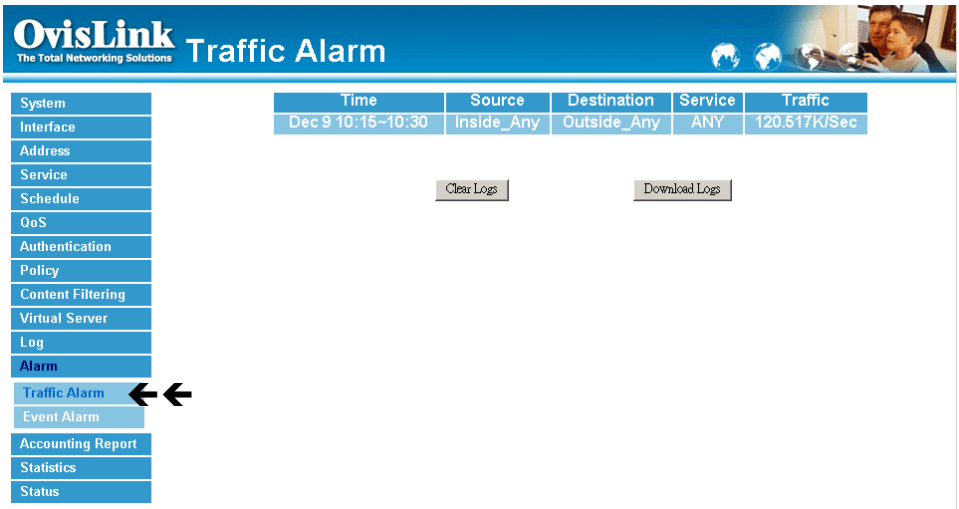


Figure11-1 Traffic Alarm

Step 2. The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- **Time:** The start and stop time of the specific connection.
- **Source:** Name of the source network of the specific connection.
- **Destination:** Name of the destination network of the specific connection.
- **Service:** Service of the specific connection.
- **Traffic:** Traffic (in Kbytes/Sec) of the specific connection.

Downloading the Traffic Alarm Logs

The Administrator can back up traffic alarm logs regularly and download it to a file on the computer.

Step 1. In the Traffic Alarm window, click the **Download Logs** button on the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.

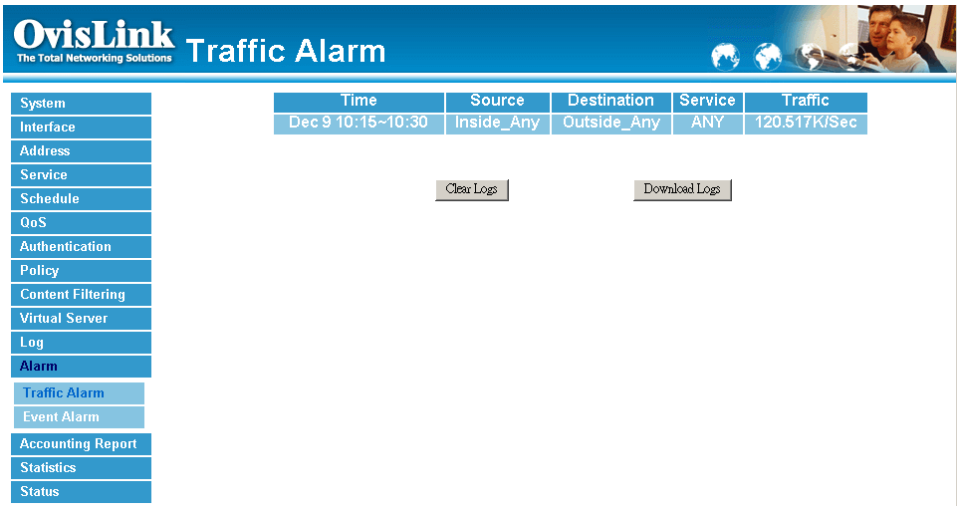


Figure11-2 Traffic Alarm

Clearing the Traffic Alarm Logs

Step 1. In the Traffic Alarm window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel.

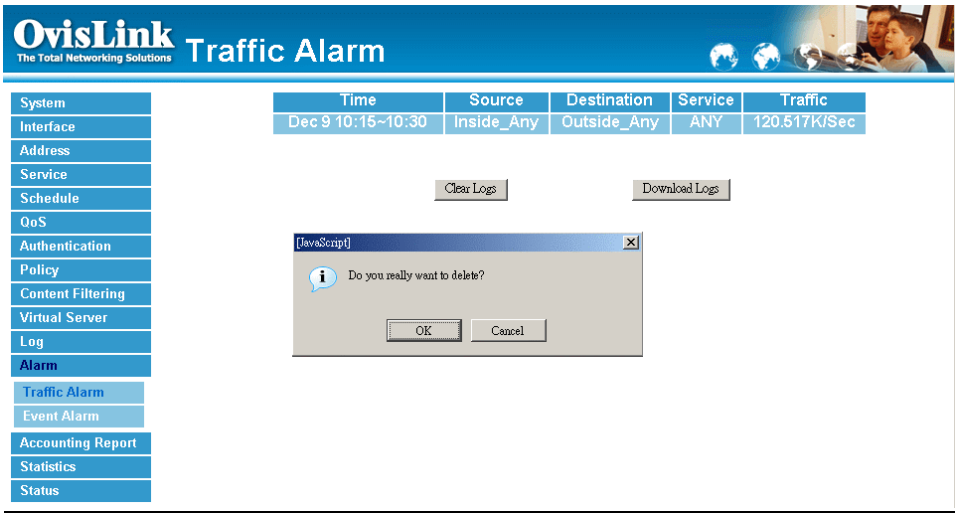


Figure11-3 Clear Traffic Alarm

Event Alarm

When Security Bandwidth Manager detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

Entering the Event Alarm window

Step 1. Click the **Event Alarm** option below the **Alarm** menu to enter the Event Alarm window.

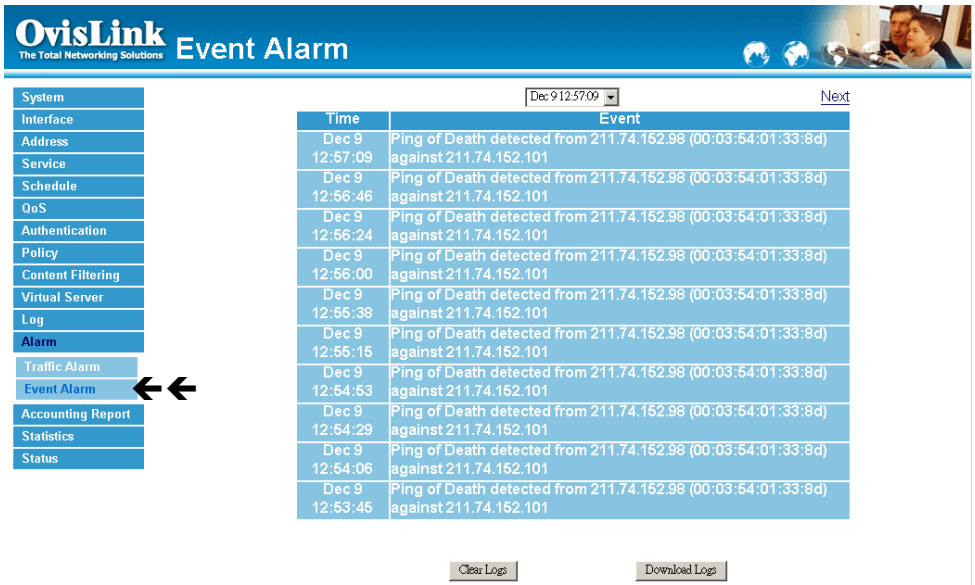


Figure11-4 Event Alarm

The table in Event Alarm window displays current traffic alarm logs for connections.

- **Time:** log time.
- **Event:** event descriptions.

Downloading the Event Alarm Logs

The Administrator can back up event alarm logs regularly by downloading it to a file on the computer.

Step 1. In the Event Alarm window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the event alarm logs into specific directory on the hard drive.

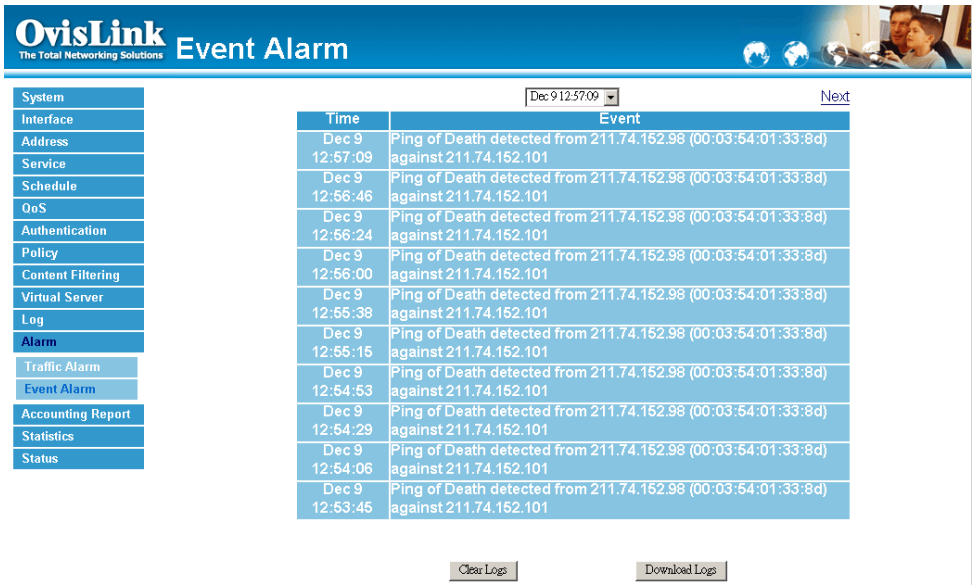


Figure11-5 Event Alarm

Clearing Event Alarm Logs

The Administrator may clear on-line logs to keep the most updated logs on the screen.

Step 1. In the Event Alarm window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK**.

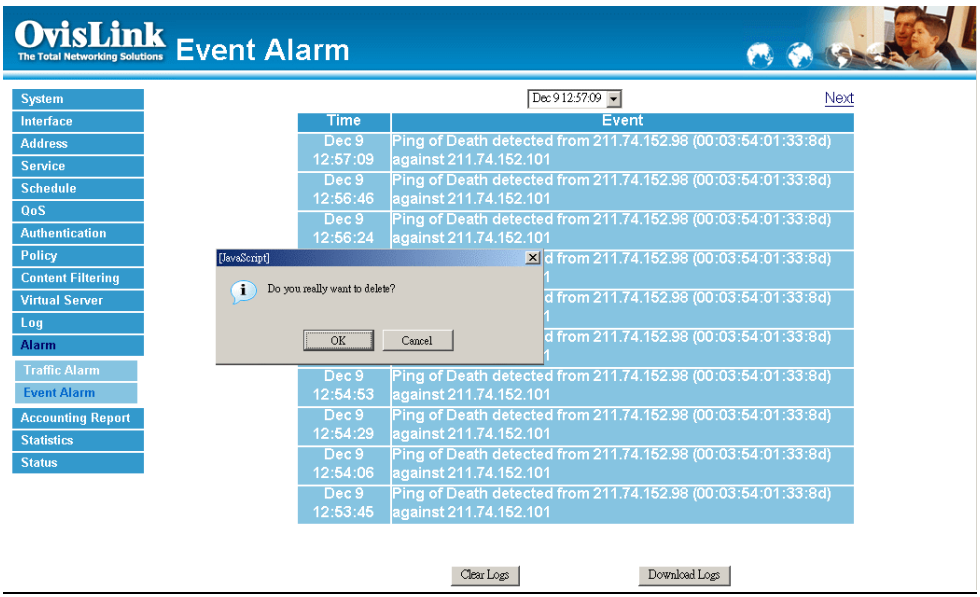


Figure11-6 Clear the Event Alarm

Accounting Report

Accounting Report can be divided into two parts, one is Outbound Accounting Report, and the other is Inbound Accounting Report.

Outbound Accounting Report

It is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication services.

Source IP：the IP address used by LAN users who use **Security Bandwidth Manager**

Destination IP：The IP address used by WAN service server which uses **Security Bandwidth Manager**.

Service：The communication service which listed in the pull-down menu when LAN users use **Security Bandwidth Manager** to connect to WAN service server.

Inbound Accounting Report

It is the statistics of downstream/upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN user uses Security Bandwidth Manager to connect to LAN Service Server.

Source IP：the IP address used by WAN users who use Security Bandwidth Manager

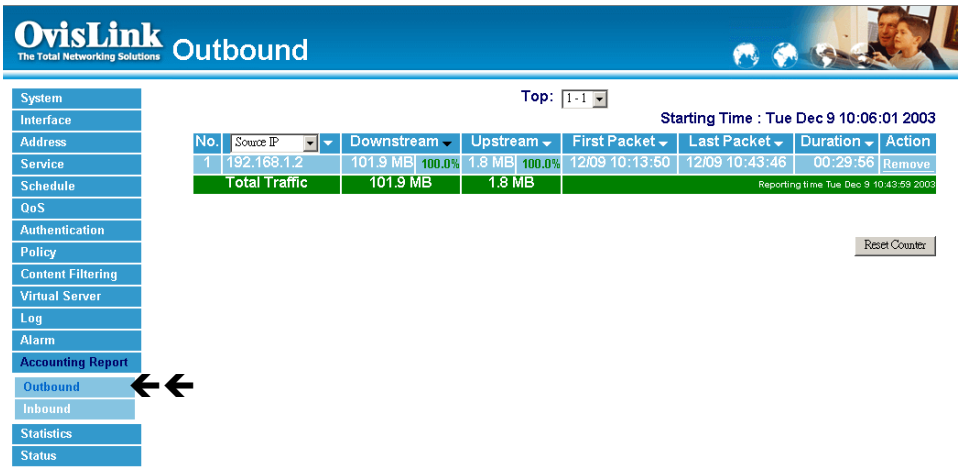
Destination IP：the IP address used by LAN service server who use Security Bandwidth Manager

Service：The communication service which listed in the pull-down menu when WAN users use Security Bandwidth Manager to connect to LAN Service server..

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service of all the user's IP that passes the Security Bandwidth Manager.

Outbound Accounting Report

Step 1. Click the **Accounting Report** function, and then select **Outbound**.



Outbound source IP Accounting Report

Source IP：When LAN users use Security Bandwidth Manager to connect to WAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the source IP will be recorded.

Definitions:

TOP：Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

Source IP：The IP address used by LAN users who use Security Bandwidth Manager to connect to WAN service server.

Downstream：The percentage of downstream and the value of each WAN service server which uses Security Bandwidth Manager to LAN user.

Upstream：The percentage of upstream and the value of each LAN user who uses Security Bandwidth Manager to WAN service server

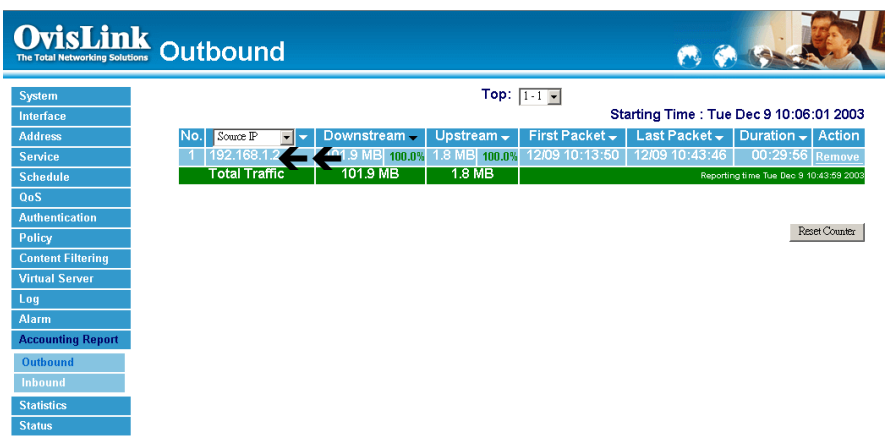
First Packet：When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the Security Bandwidth Manager.

Last Packet：When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the Security Bandwidth Manager.

Duration：The period of time which starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.

Reset Counter：Click **Reset Counter** button to refresh Accounting Report.



Outbound Destination IP Accounting Report

Destination IP：When WAN service server uses Security Bandwidth Manager to connect to LAN user, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Definition:

TOP：Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

Destination IP：The IP address used by WAN service server which uses Security Bandwidth Manager.

Downstream：The percentage of downstream and the value of each WAN service server which uses Security Bandwidth Manager to LAN user.

Upstream：The percentage of upstream and the value of each LAN user who uses Security Bandwidth Manager to WAN service server.

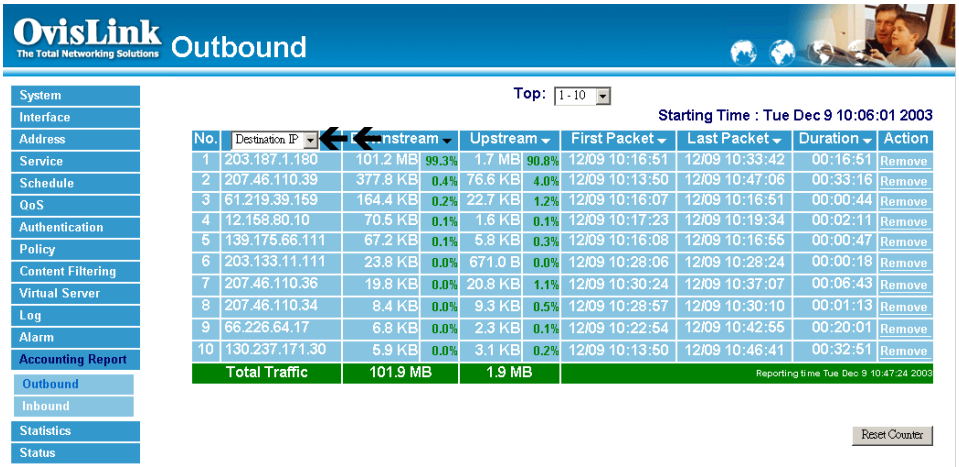
First Packet：When the first packet is sent from WAN service server to LAN users, the sent time will be recorded by the Security Bandwidth Manager.

Last Packet：When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the Security Bandwidth Manager.

Duration：The period of time which starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of time and show the percentage of each WAN service server’s upstream/downstream to LAN user.

Reset Counter：Click **Reset Counter** button to refresh Accounting Report.


OvisLink
The Total Networking Solutions
Outbound
System
Interface
Address
Service
Schedule
QoS
Authentication
Policy
Content Filtering
Virtual Server
Log
Alarm
Accounting Report
Outbound
Inbound
Statistics
Status
Top: 1 - 10
Starting Time : Tue Dec 9 10:06:01 2003
No. Destination IP Downstream Upstream First Packet Last Packet Duration Action
1 203.187.1.180 101.2 MB 99.3% 1.7 MB 90.8% 12/09 10:16:51 12/09 10:33:42 00:16:51 Remove
2 207.46.110.39 377.8 KB 0.4% 76.6 KB 4.0% 12/09 10:13:50 12/09 10:47:06 00:33:16 Remove
3 61.219.39.159 164.4 KB 0.2% 22.7 KB 1.2% 12/09 10:16:07 12/09 10:16:51 00:00:44 Remove
4 12.158.80.10 70.5 KB 0.1% 1.6 KB 0.1% 12/09 10:17:23 12/09 10:19:34 00:02:11 Remove
5 139.175.66.111 67.2 KB 0.1% 5.8 KB 0.3% 12/09 10:16:08 12/09 10:16:55 00:00:47 Remove
6 203.133.11.111 23.8 KB 0.0% 671.0 B 0.0% 12/09 10:28:06 12/09 10:28:24 00:00:18 Remove
7 207.46.110.36 19.8 KB 0.0% 20.8 KB 1.1% 12/09 10:30:24 12/09 10:37:07 00:06:43 Remove
8 207.46.110.34 8.4 KB 0.0% 9.3 KB 0.5% 12/09 10:28:57 12/09 10:30:10 00:01:13 Remove
9 66.226.64.17 6.8 KB 0.0% 2.3 KB 0.1% 12/09 10:22:54 12/09 10:42:55 00:20:01 Remove
10 130.237.171.30 5.9 KB 0.0% 3.1 KB 0.2% 12/09 10:13:50 12/09 10:46:41 00:32:51 Remove
Total Traffic 101.9 MB 1.9 MB
Reporting time Tue Dec 9 10:47:24 2003
Reset Counter

Outbound Service Accounting Report

Service： When LAN users use Security Bandwidth Manager to connect to WAN Service Server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Definitions:

TOP：Select the data you want to view. It presents 10 results in one page.

：According to the downstream/upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

Pull-down menu selection

Service：The report of Communication Service when LAN users use the Security Bandwidth Manager to connect to WAN service server.

Downstream：The percentage of downstream and the value of each WAN service server who uses Security Bandwidth Manager to connect to LAN user.

Upstream：The percentage of upstream and the value of each LAN user who uses Security Bandwidth Manager to WAN service server.

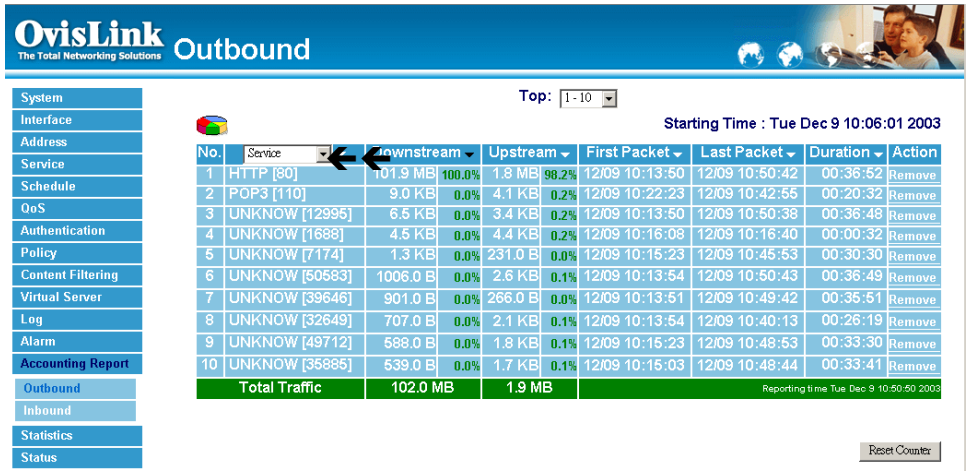
First Packet：When the first packet is sent to the WAN Service Server, the sent time will be recorded by the Security Bandwidth Manager.

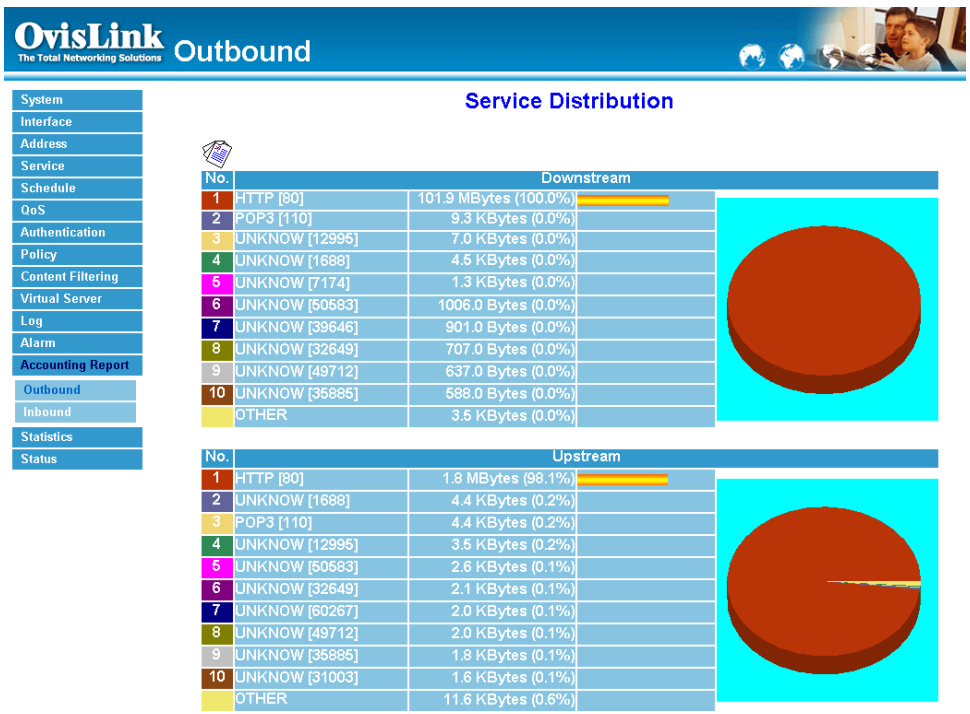
Last Packet：When the last packet is sent from the WAN Service Server, the sent time will be recorded by the Security Bandwidth Manager

Duration：The period of time starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server..

Reset Counter：Click the Reset Counter button to refresh the Accounting Report.

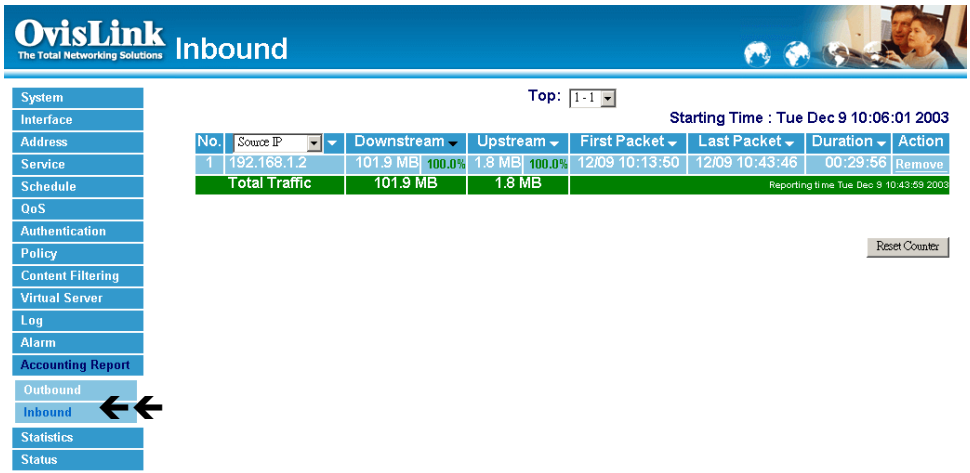

OvisLink
The Total Networking Solutions
Outbound
System
Interface
Address
Service
Schedule
QoS
Authentication
Policy
Content Filtering
Virtual Server
Log
Alarm
Accounting Report
Outbound
Inbound
Statistics
Status
Top: 1 - 10
Starting Time : Tue Dec 9 10:06:01 2003
No. Service Downstream Upstream First Packet Last Packet Duration Action
1 HTTP [80] 101.9 MB 100.0% 1.8 MB 98.2% 12/09 10:13:50 12/09 10:50:42 00:36:52 Remove
2 POP3 [110] 9.0 KB 0.0% 4.1 KB 0.2% 12/09 10:22:23 12/09 10:42:55 00:20:32 Remove
3 UNKNOW [12995] 6.5 KB 0.0% 3.4 KB 0.2% 12/09 10:13:50 12/09 10:50:38 00:36:48 Remove
4 UNKNOW [1688] 4.5 KB 0.0% 4.4 KB 0.2% 12/09 10:16:08 12/09 10:16:40 00:00:32 Remove
5 UNKNOW [7174] 1.3 KB 0.0% 231.0 B 0.0% 12/09 10:15:23 12/09 10:45:53 00:30:30 Remove
6 UNKNOW [50583] 1006.0 B 0.0% 2.6 KB 0.1% 12/09 10:13:54 12/09 10:50:43 00:36:49 Remove
7 UNKNOW [39646] 901.0 B 0.0% 266.0 B 0.0% 12/09 10:13:51 12/09 10:49:42 00:35:51 Remove
8 UNKNOW [32649] 707.0 B 0.0% 2.1 KB 0.1% 12/09 10:13:54 12/09 10:40:13 00:26:19 Remove
9 UNKNOW [49712] 588.0 B 0.0% 1.8 KB 0.1% 12/09 10:15:23 12/09 10:48:53 00:33:30 Remove
10 UNKNOW [35885] 539.0 B 0.0% 1.7 KB 0.1% 12/09 10:15:03 12/09 10:48:44 00:33:41 Remove
Total Traffic 102.0 MB 1.9 MB
Reporting time Tue Dec 9 10:50:50 2003
Reset Counter



Press to return to **Accounting Report** window.

Inbound

Step 1. Click **Service** in the menu bar on the left hand side of the window. Click **Group** under it.



Inbound Source IP Accounting Report

Source IP：When WAN users use Security Bandwidth Manager to connect to LAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the source IP will be recorded.

Definitions:

TOP：Select the data you want to view. It presents 10 pages in one page.
Select from the Pull-down menu

Source IP：The IP address used by WAN users who use Security Bandwidth Manager.

Downstream：The percentage of Downstream and the value of each WAN user who uses Security Bandwidth Manager to LAN service server.

Upstream：The percentage of Upstream and the value of each LAN service server who uses Security Bandwidth Manager to WAN users.

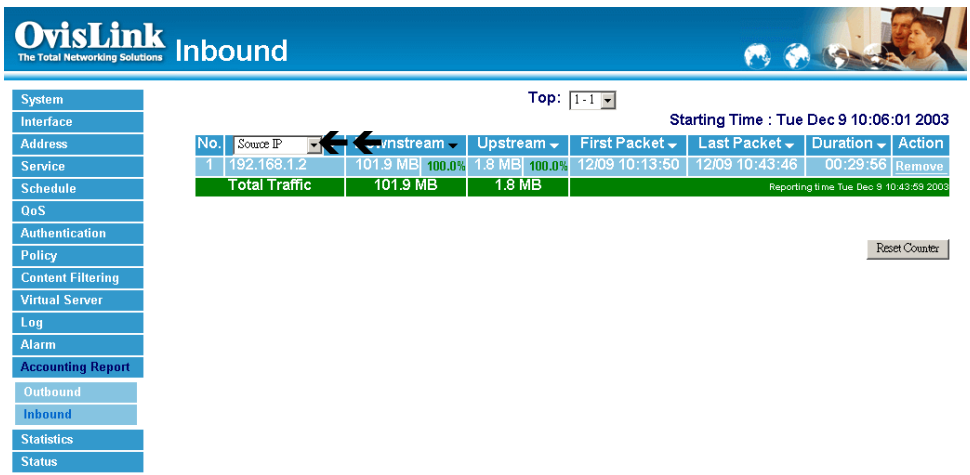
First Packet：When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the Security Bandwidth Manager.

Last Packet：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the Security Bandwidth Manager..

Duration：The period of time starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of time and show the percentage of each WAN user's upstream/downstream to LAN service server.

Reset Counter：Click the **Reset Counter** button to refresh the Accounting Report.



Inbound Destination IP Accounting Report

Destination IP：When WAN users use Security Bandwidth Manager to connect to LAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Definitions:

TOP：Select the data you want to view. It presents 10 pages in one page.

Pull-down menu selection

Destination IP：The IP address used by WAN users who uses Security Bandwidth Manager.

Downstream：The percentage of Downstream and the value of each WAN user who uses Security Bandwidth Manager to LAN service server.

Upstream：The percentage of Upstream and the value of each LAN service server who uses Security Bandwidth Manager to WAN users.

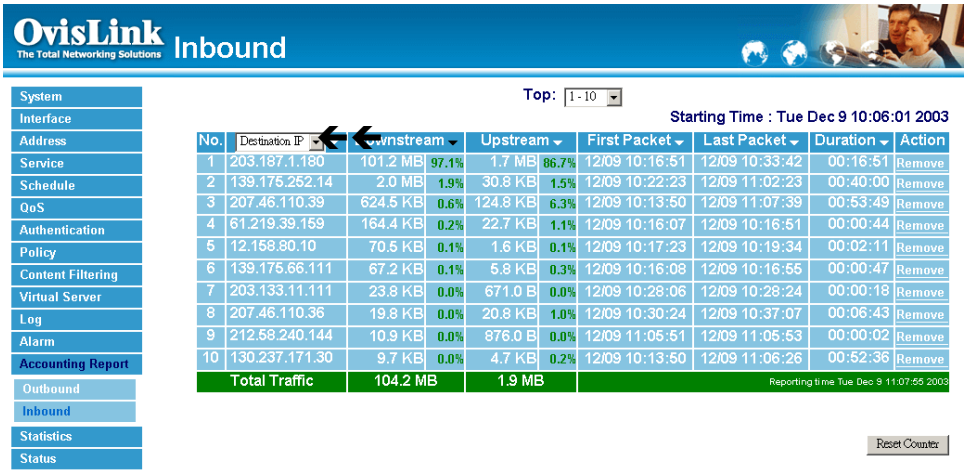
First Packet：When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the Security Bandwidth Manager.

Last Packet：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the Security Bandwidth Manager..

Duration：The period of time starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of time and show the percentage of each WAN user’s upstream/downstream to LAN service server.

Reset Counter：Click the **Reset Counter** button to refresh the Accounting Report.


OvisLink
The Total Networking Solutions
Inbound
System
Interface
Address
Service
Schedule
QoS
Authentication
Policy
Content Filtering
Virtual Server
Log
Alarm
Accounting Report
Outbound
Inbound
Statistics
Status
Top: 1 - 10
Starting Time : Tue Dec 9 10:06:01 2003
No. Destination IP Downstream Upstream First Packet Last Packet Duration Action
1 203.187.1.180 101.2 MB 97.1% 1.7 MB 86.7% 12/09 10:16:51 12/09 10:33:42 00:16:51 Remove
2 139.175.252.14 2.0 MB 1.9% 30.8 KB 1.5% 12/09 10:22:23 12/09 11:02:23 00:40:00 Remove
3 207.46.110.39 624.5 KB 0.6% 124.8 KB 6.3% 12/09 10:13:50 12/09 11:07:39 00:53:49 Remove
4 61.219.39.159 164.4 KB 0.2% 22.7 KB 1.1% 12/09 10:16:07 12/09 10:16:51 00:00:44 Remove
5 12.158.80.10 70.5 KB 0.1% 1.6 KB 0.1% 12/09 10:17:23 12/09 10:19:34 00:02:11 Remove
6 139.175.66.111 67.2 KB 0.1% 5.8 KB 0.3% 12/09 10:16:08 12/09 10:16:55 00:00:47 Remove
7 203.133.11.111 23.8 KB 0.0% 671.0 B 0.0% 12/09 10:28:06 12/09 10:28:24 00:00:18 Remove
8 207.46.110.36 19.8 KB 0.0% 20.8 KB 1.0% 12/09 10:30:24 12/09 10:37:07 00:06:43 Remove
9 212.58.240.144 10.9 KB 0.0% 876.0 B 0.0% 12/09 11:05:51 12/09 11:05:53 00:00:02 Remove
10 130.237.171.30 9.7 KB 0.0% 4.7 KB 0.2% 12/09 10:13:50 12/09 11:06:26 00:52:36 Remove
Total Traffic 104.2 MB 1.9 MB
Reporting time Tue Dec 9 11:07:55 2003
Reset Counter

Inbound Service Accounting Report

Service： When WAN users use **Security Bandwidth Manager** to connect to LAN Service Server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Definitions:

TOP：Select the data you want to view. It presents 10 results in one page.

：According to the downstream/upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

Pull-down menu selection

Service：The report of Communication Service when WAN users use the Security Bandwidth Manager to connect to LAN service server.

Downstream：The percentage of downstream and the value of each WAN user who uses Security Bandwidth Manager to LAN service server.

Upstream：The percentage of upstream and the value of each LAN service server who uses Security Bandwidth Manager to WAN user.

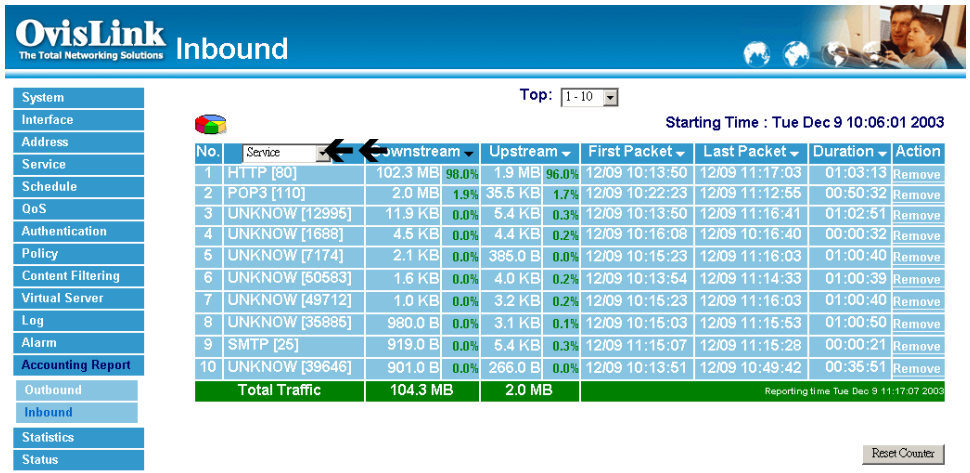
First Packet：When the first packet is sent to the LAN Service Server, the sent time will be recorded by the Security Bandwidth Manager.

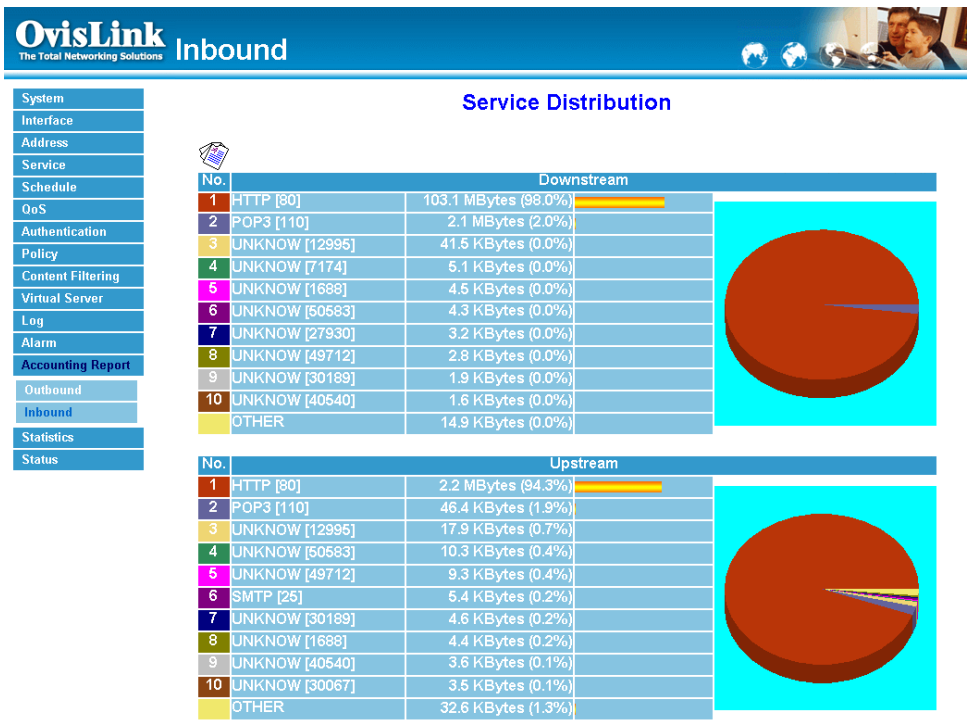
Last Packet：When the last packet is sent from the LAN Service Server, the sent time will be recorded by the Security Bandwidth Manager

Duration：The period of time starts from the first packet to the last packet to be recorded.

Total Traffic：The Security Bandwidth Manager will record the sum of time and show the percentage of each Communication Service's upstream/downstream to LAN service server..

Reset Counter：Click the **Reset Counter** button to refresh the Accounting Report.


OvisLink
The Total Networking Solutions
Inbound
System
Interface
Address
Service
Schedule
QoS
Authentication
Policy
Content Filtering
Virtual Server
Log
Alarm
Accounting Report
Outbound
Inbound
Statistics
Status
Top: 1 - 10
Starting Time : Tue Dec 9 10:06:01 2003
No. Service Downstream Upstream First Packet Last Packet Duration Action
1 HTTP [80] 102.3 MB 98.0% 1.9 MB 96.0% 12/09 10:13:50 12/09 11:17:03 01:03:13 Remove
2 POP3 [110] 2.0 MB 1.9% 35.5 KB 1.7% 12/09 10:22:23 12/09 11:12:55 00:50:32 Remove
3 UNKNOW [12995] 11.9 KB 0.0% 5.4 KB 0.3% 12/09 10:13:50 12/09 11:16:41 01:02:51 Remove
4 UNKNOW [1688] 4.5 KB 0.0% 4.4 KB 0.2% 12/09 10:16:08 12/09 10:16:40 00:00:32 Remove
5 UNKNOW [7174] 2.1 KB 0.0% 385.0 B 0.0% 12/09 10:15:23 12/09 11:16:03 01:00:40 Remove
6 UNKNOW [50583] 1.6 KB 0.0% 4.0 KB 0.2% 12/09 10:13:54 12/09 11:14:33 01:00:39 Remove
7 UNKNOW [49712] 1.0 KB 0.0% 3.2 KB 0.2% 12/09 10:15:23 12/09 11:16:03 01:00:40 Remove
8 UNKNOW [35885] 980.0 B 0.0% 3.1 KB 0.1% 12/09 10:15:03 12/09 11:15:53 01:00:50 Remove
9 SMTP [25] 919.0 B 0.0% 5.4 KB 0.3% 12/09 11:15:07 12/09 11:15:28 00:00:21 Remove
10 UNKNOW [39646] 901.0 B 0.0% 266.0 B 0.0% 12/09 10:13:51 12/09 10:49:42 00:35:51 Remove
Total Traffic 104.3 MB 2.0 MB Reporting time Tue Dec 9 11:17:07 2003
Reset Counter



Press and return to **Accounting Report** window.

Statistics

In this chapter, the Administrator queries the Security Bandwidth Manager for statistics of packets and data which passes across the Security Bandwidth Manager. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the Security Bandwidth Manager by control policies setup by the Administrator.

How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to mange networks.

How to apply WAN Statistics

The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics, in this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

The administrator needs to go to the Policy to set the network IP of the WAN statistics. By the Wan statistics you can obtain the status of the network.

WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN Statistics.

Step 2. The WAN Statistics will be displayed.

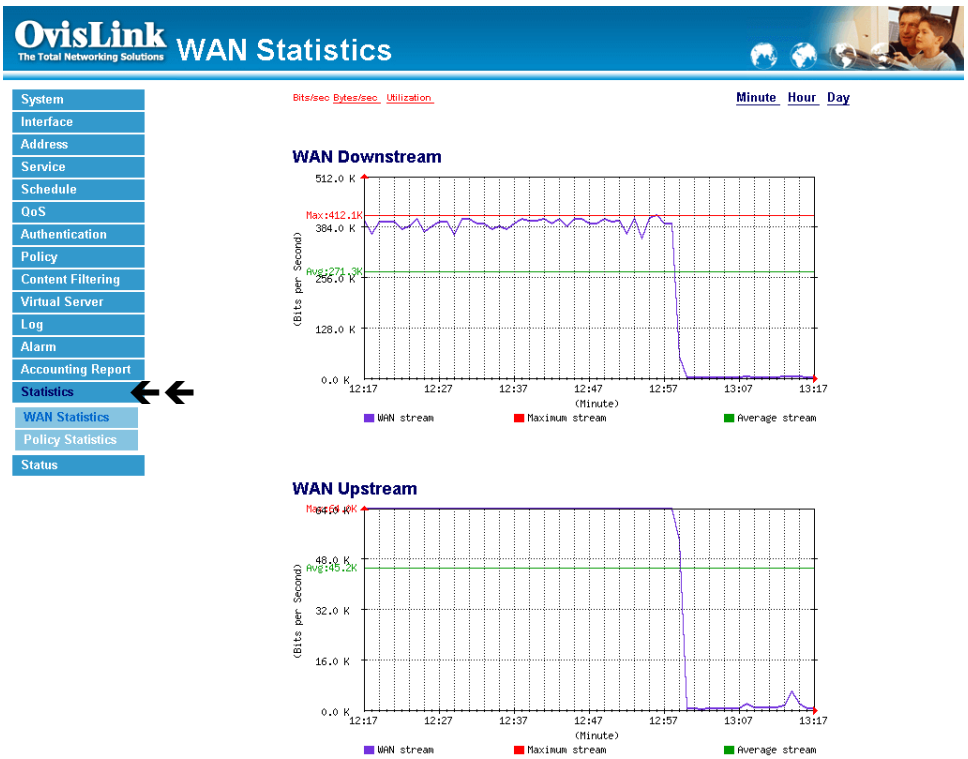


Figure13-1 WAN Statistics

Time：The statistics based on the units of minute, hour and day.

WAN Downstream Figure

WAN Upstream Figure

WAN Downstream Packet Figure

WAN upstream Packet Figure

WAN Statistics

Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

Step 2. In Statistics window, find the domain name you want to view.

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate：Network Traffic（Kbytes/Sec）.

X-Coordinate：Time（Hour/Minute/Day）.

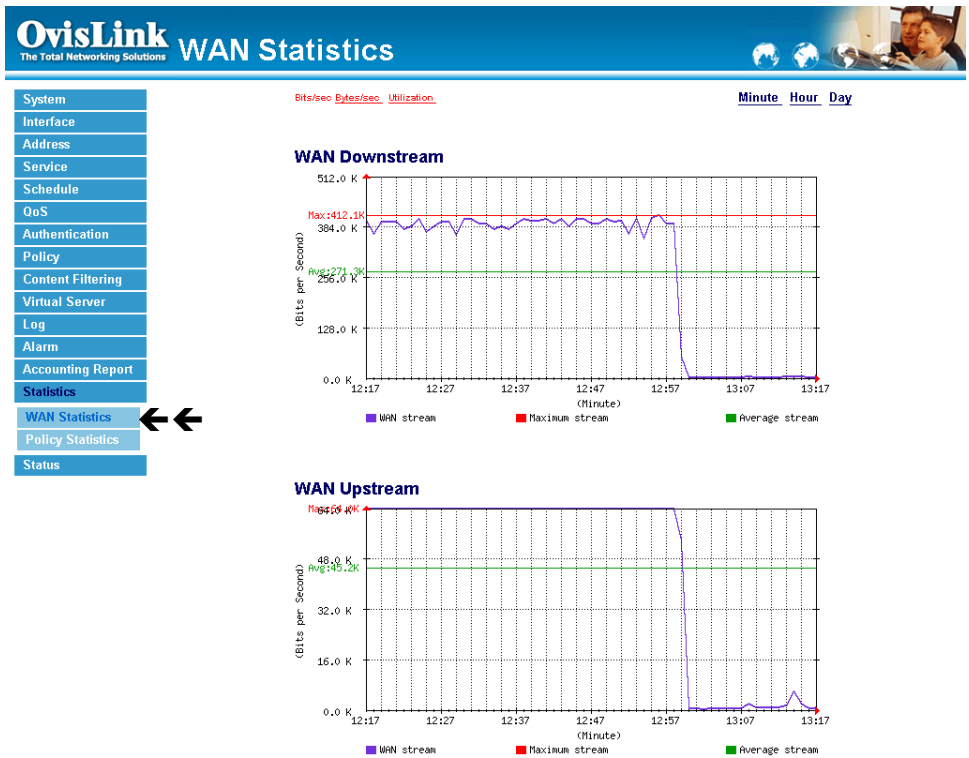


Figure13-2 WAN Sttatistics

Policy Statistics

Entering the Statistics window

Step 1. The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, or days

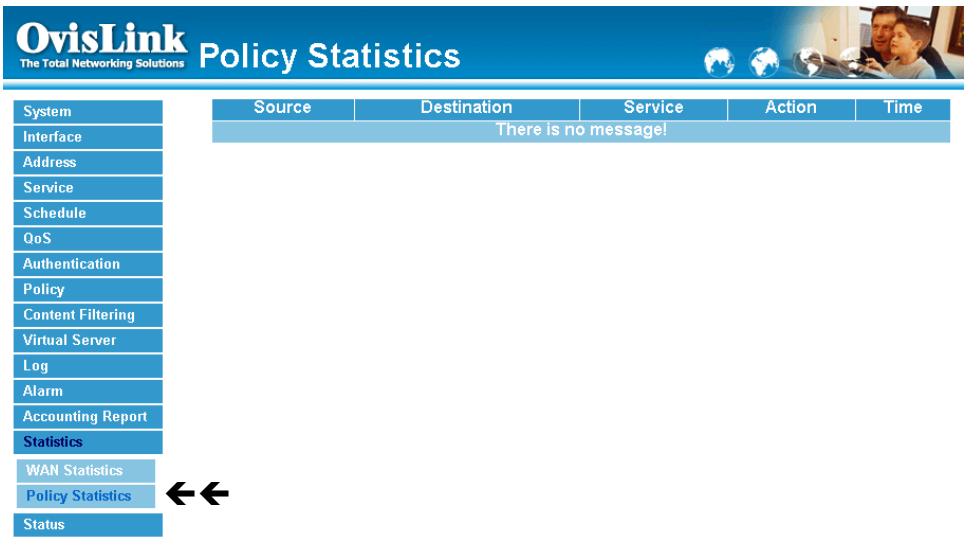


Figure13-3 Policy Statistics

To use Statistics, the administrator needs to go to Policy to enable Statistics function.

Entering the Policy Satistics

Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

Step 2. In Statistics window, find the domain name you want to view

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate：Network Traffic（Kbytes/Sec）。

X-Coordinate：Time（Hour/Minute/Day）。

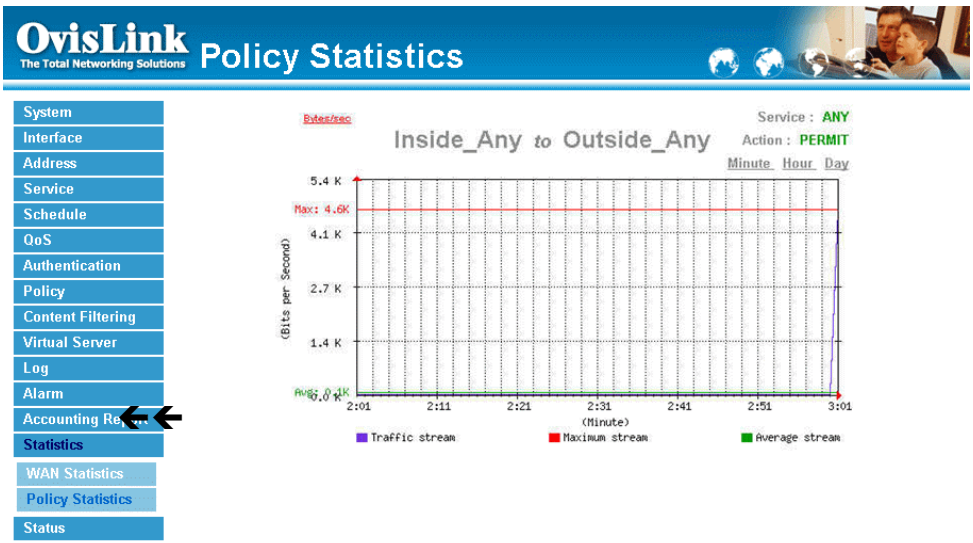


Figure13-4 Checking Policy Statistics

Status

In this section, the device displays the status information about the Security Bandwidth Manager. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Security Bandwidth Manager.

Interface Status

Entering the Interface Status window

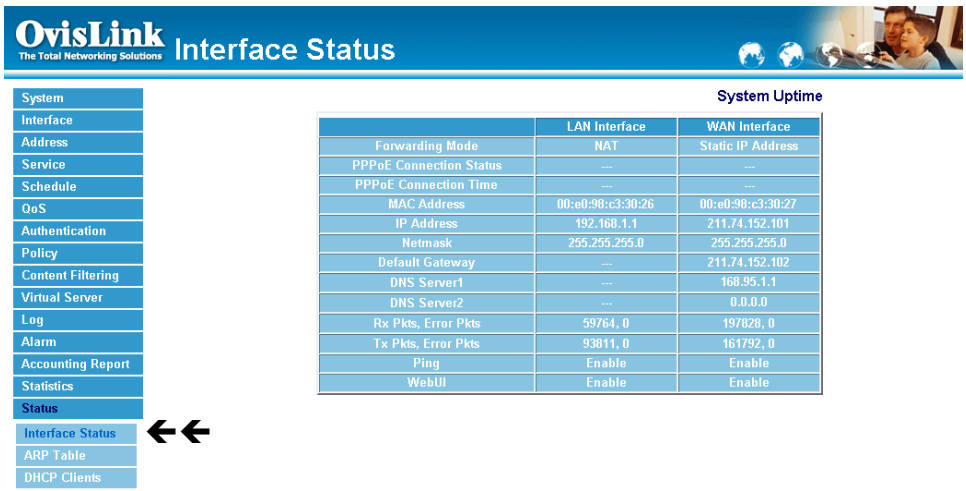


Figure14-1 Interface Status

Internal Interface

In Internet Interface window: The interface IP will be displayed.

System Uptime：The time of booting the Security Bandwidth Manager.

Forwarding Mode：NAT mode or Transparent mode.

MAC Address：The serial number of the network card.

IP Address/Netmask: Internal IP Address/Internal Netmask

Rx Pkts, Error Pkts：The received packets and the error received packets will be shown.

Tx Pkts, Error Pkts：The transmit packets and the error transmit packets will be shown.

ADSL Static IP or Cable Modem users

Forwarding Mode：NAT mode or Transparent mode.

Connection Status：Displays the connection status of LAN network.

Connection Time：Displays the connection time of LAN network.

MAC Address：The serial number of the network card.

IP Address/Netmask: external IP Address/external Netmask

Default Gateway：Displays the WAN Gateway address.

Rx Pkts, Error Pkts：The received packets and the error received packets will be shown.

Tx Pkts, Error Pkts：The transmit packets and the error transmit packets will be shown.

DNS Server 1：Displays the using DNS Server 1

DNS Server 2：Displays the using DNS Server 2.

ARP Table

Entering the ARP Table window

Step 1. Click on **Status** in the menu bar, then click **ARP Table** below it.

Step 2. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN network that replies to an ARP packet, the device will list them in this ARP table.

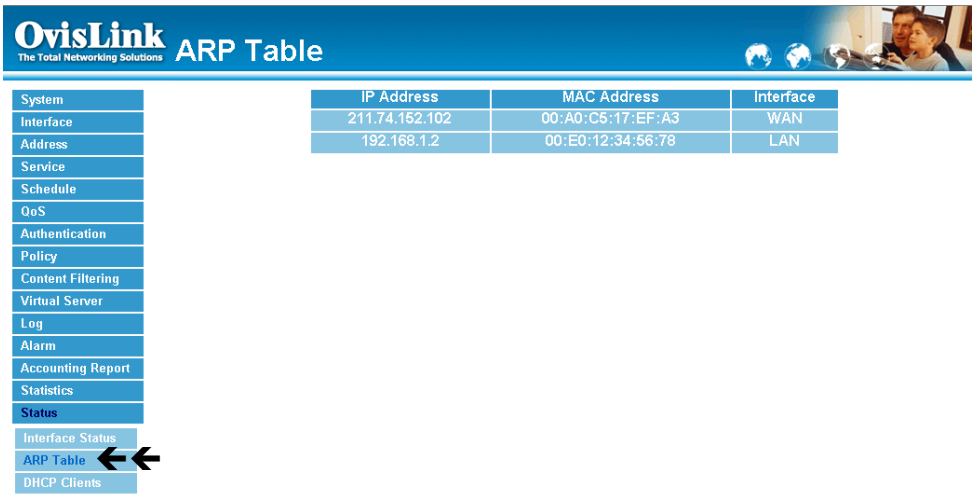


Figure14-3 ARP Table

IP Address: The IP address of the host computer

MAC Address: The MAC address of that host computer

Interface: The port that the host computer is connected to (LAN, WAN)

DHCP Clients

Entering the DHCP Clients window

Step 1. Click on **Status** in the menu bar, then click on **DHCP Clients** below it.

Step 2. A window will appear displaying the table of DHCP clients that are connected to the device. The table will list host computers on the LAN network that obtain its IP address from the Bandwidth Manager's DHCP server function.

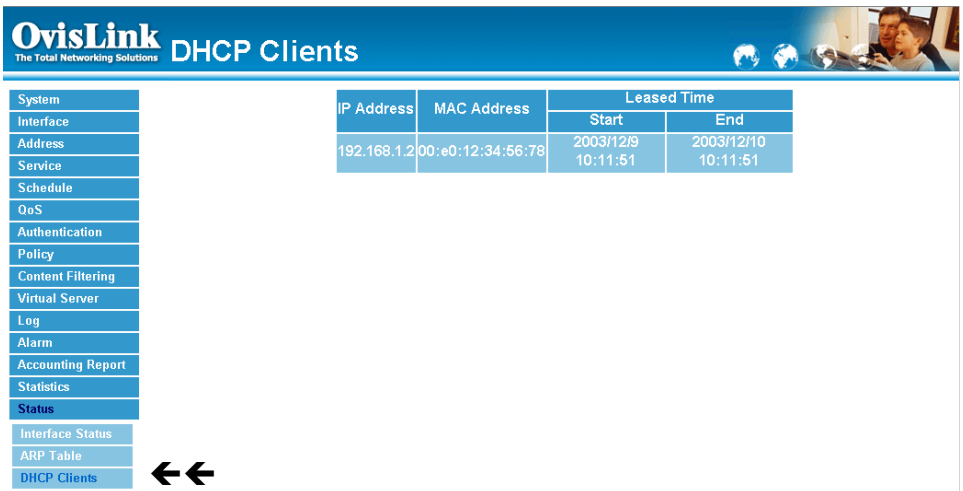


Figure14-4 DHCP Clients

IP Address: the IP address of the LAN host computer

MAC Address: MAC address of the LAN host computer

Leased Time: The Start and End time of the DHCP lease for the LAN host computer.

Setup Examples

Example 1: Allow the LAN network to be able to access the Internet

Example 2: The LAN network can only access Yahoo.com website

Example 3: Outside users can access the LAN FTP server through Virtual Servers

Example 4: I Install a server inside the LAN network and have the Internet (WAN) users access the server through IP Mapping

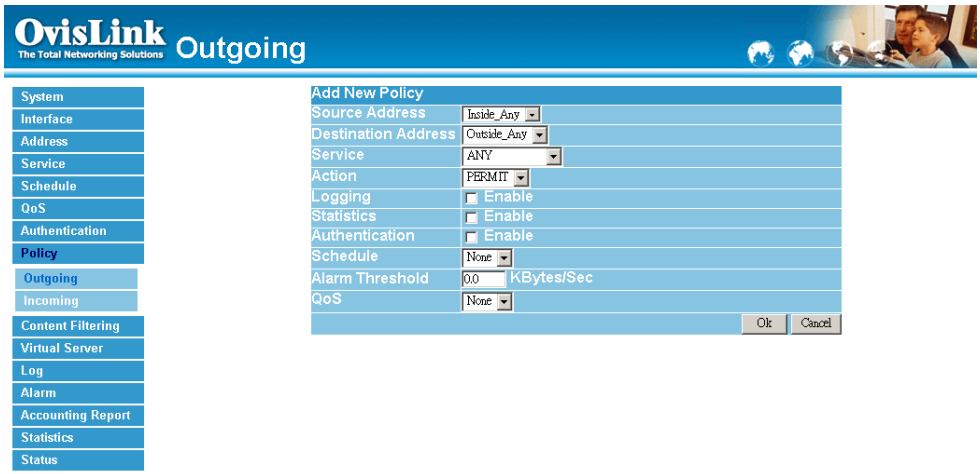
Example 5: Use QoS to setup LAN to WAN network to attain the maximum downstream/upstream bandwidth. The setup orders should be QoS and then Policy

Example 1: Allow the LAN network to be able to access the Internet

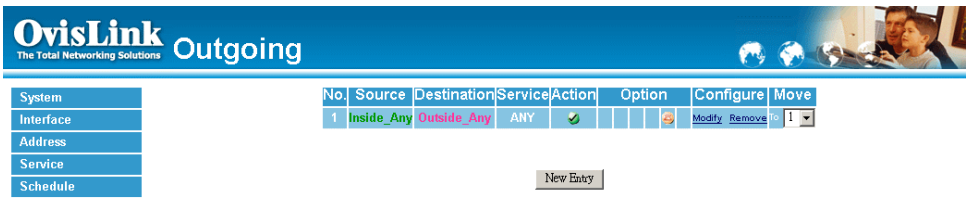
Step 1. Enter the Outgoing window under the Policy menu.

Step 2. Click the **New Entry** button on the bottom of the screen.

Step 3. In the Add New Policy window, enter each parameter, then click OK.



Step 4 When the following screen appears, the setup is completed.

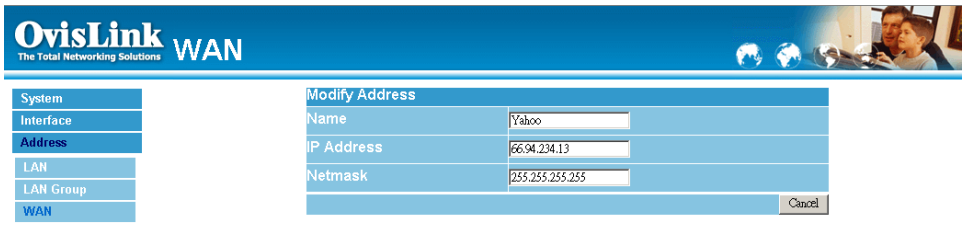


Example 2: **The LAN network can only access Yahoo.com website.**

Step 1. Enter the WAN window under the Address menu.

Step 2. Click the **New Entry** button.

Step 3. In the Add New Address window, enter relating parameters.

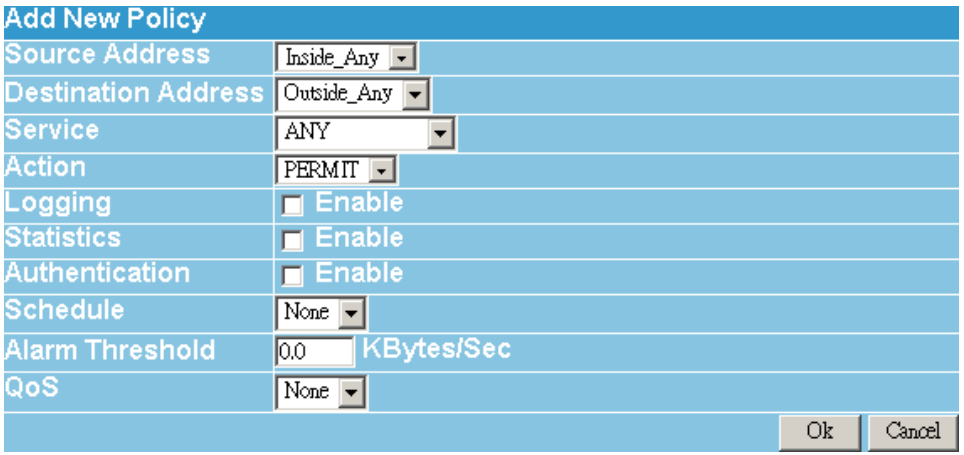


Step 4. Click **OK** to end the address table setup.

Step 5. Go to the **Outgoing** window under the Policy menu.

Step 6. Click the **New Entry** button.

Step 7. In the **Add New Policy** window, enter corresponding parameters. Click **OK**.



Step 8. When the following screen appears, the setup is completed.

No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1
2	Inside_Any	yahoo	ANY	✓		Modify Remove	To 2

New Entry

Example 3:Outside users can access the LAN FTP server through Virtual Servers

Step 1. Enter Virtual Server under the Virtual Server menu.

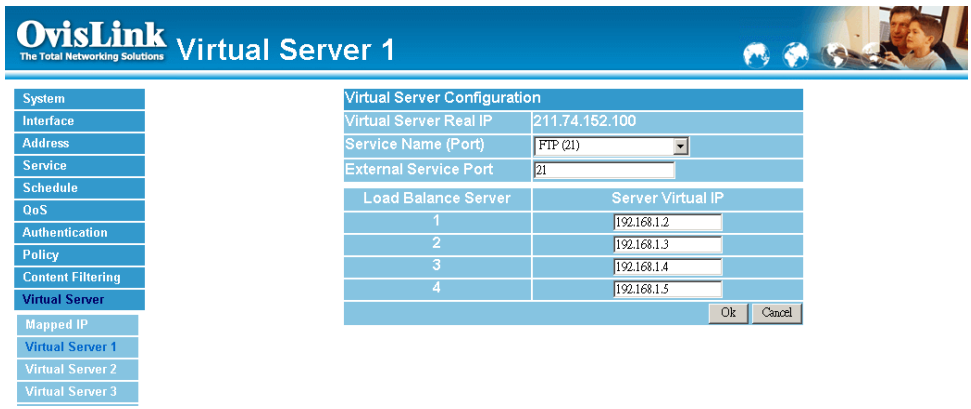
Step 2. Click the ‘click here to configure’ button.

Step 3. Select an WANIP address, then click OK.

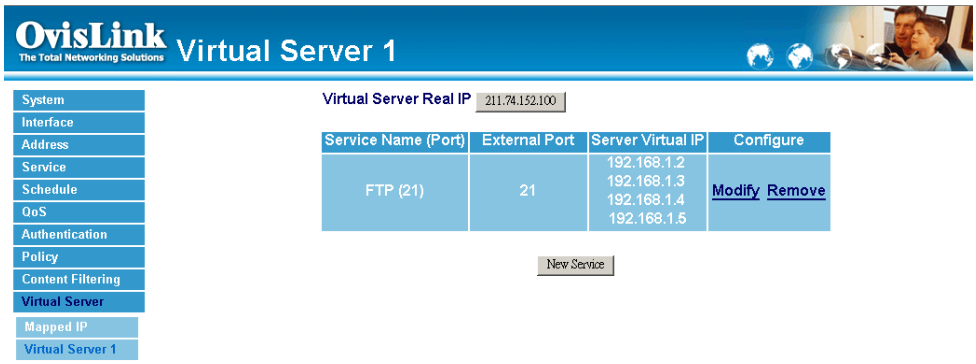
Step 4. Click the New Service button on the bottom of the screen.

Step 5. Add the FTP service pointing to the LAN server IP address.

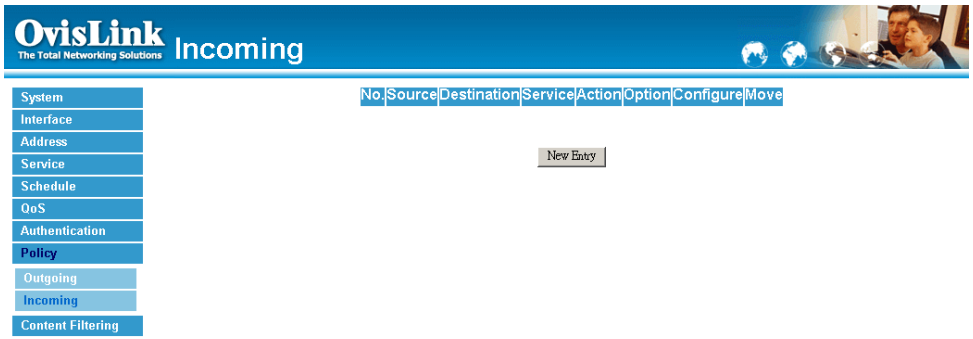
Step 6. Click OK.



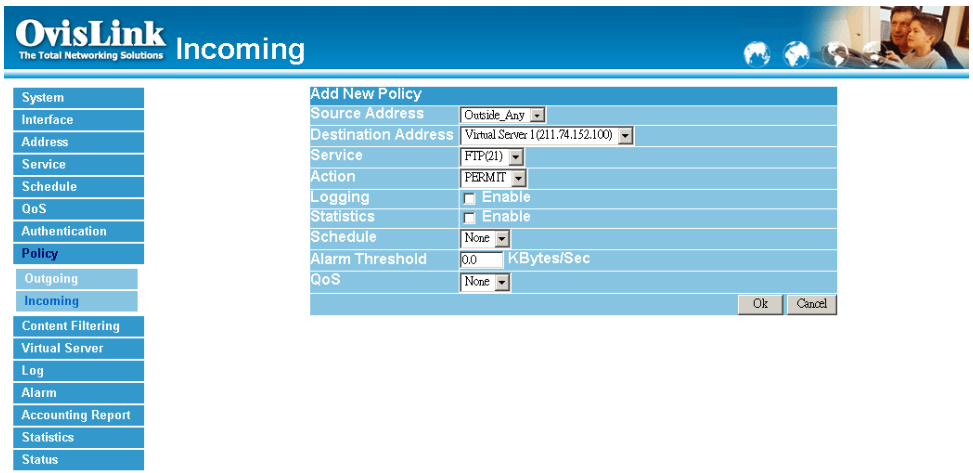
Step 7. A new Virtual Service should appear.



Step 8. Go to the Incoming window under the Policy menu, then click on the **New Entry** button.



Step 9.In the **Add New Policy** window, set each parameter, then click OK.



Step 10. An Incoming FTP policy should now be created.

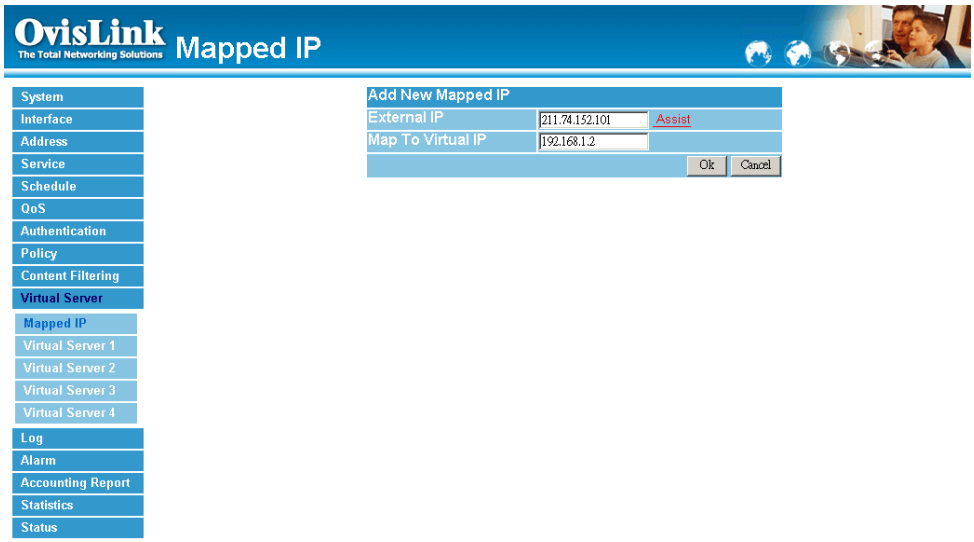
Example 4: Install a server inside the LAN network and have the Internet (WAN) users access the server through IP Mapping

Step 1. Enter the Mapped IP window under the Virtual Server menu.

Step 2. Click the **New Entry** button.

Step 3. In the Add New IP Mapping window, enter each parameter.

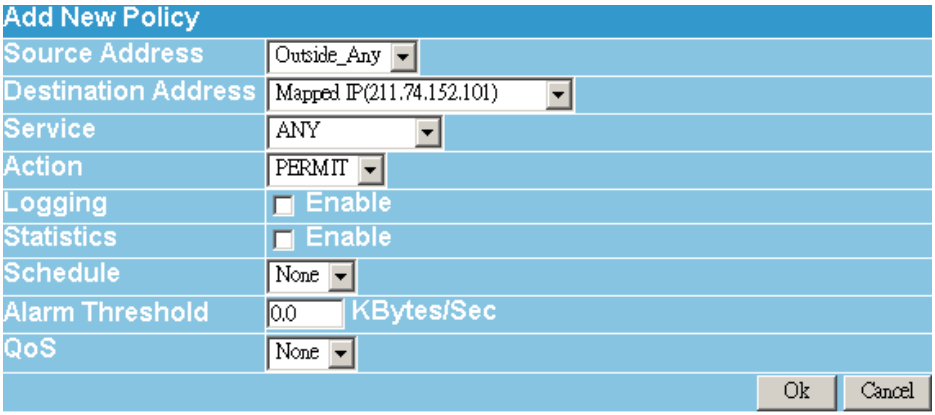
Step 4. Click **OK**.



Step 3. When the following screen appears, the IP Mapping setup is completed.

Step 4. Go to the Incoming window under the Policy menu.

Step 5. Click the **New Entry** button.



Step 6. In the **Add New Policy** window, set each parameter, then click **OK**.

Step 7. Open all the services. (ANY)

Step 8. The setup is completed.

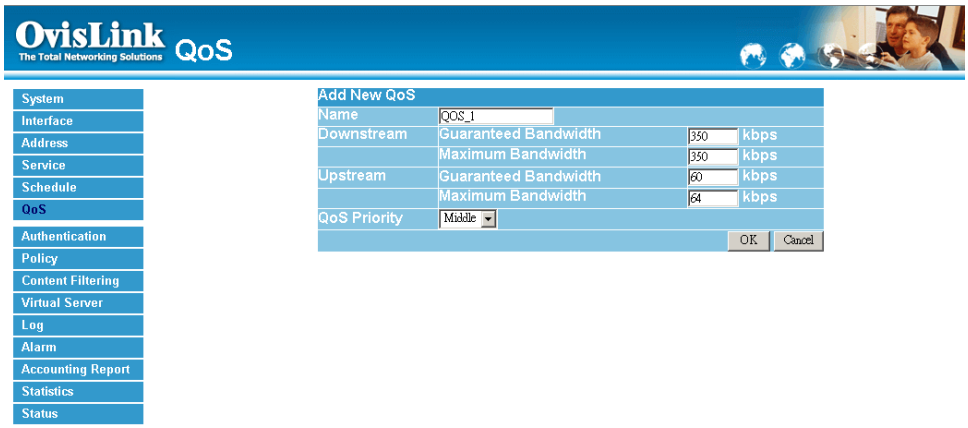
Example 5: Use QoS to setup LAN to WAN network to attain the maximum downstream/upstream bandwidth. The setup orders should be QoS and then Policy

Step 1. Enter the **QoS** window in the menu bar on the left hand side of the window.

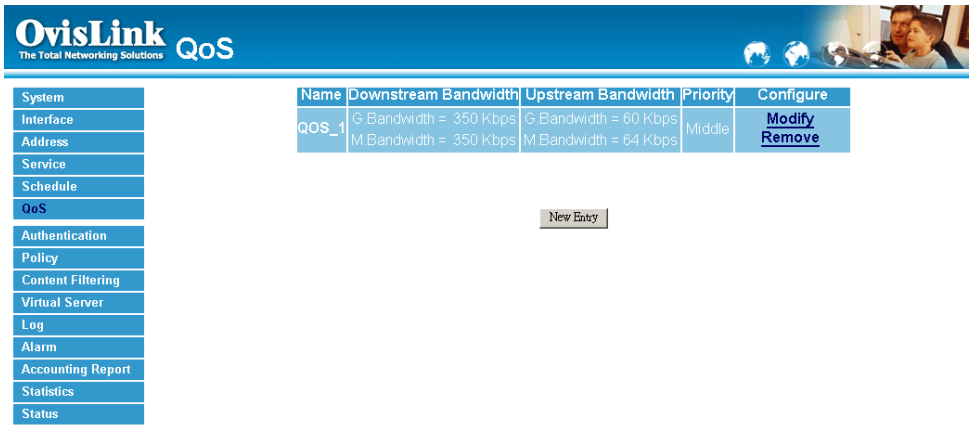
Step 2. Click the **New Entry** button.

Step 3. In the **Add New QoS** window, enter each parameter.

Step 4. Click **OK**.



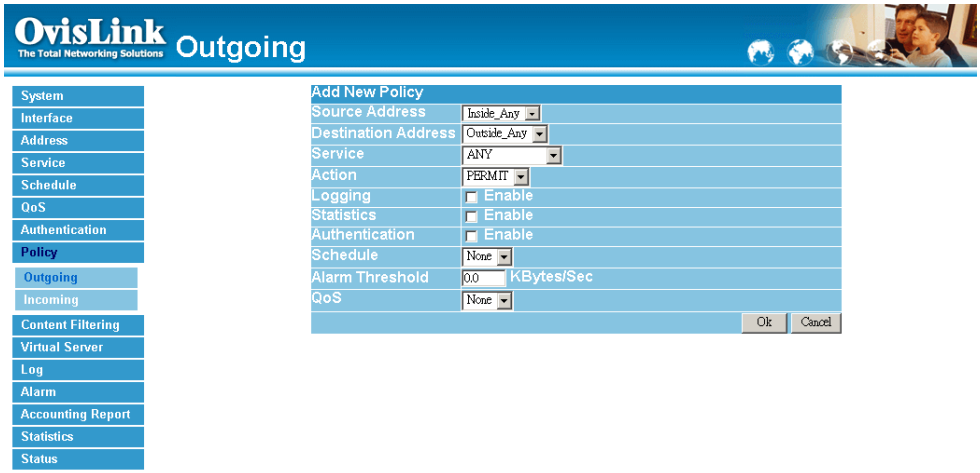
Step 5. When the following screen appears, the **QoS** setup is completed.



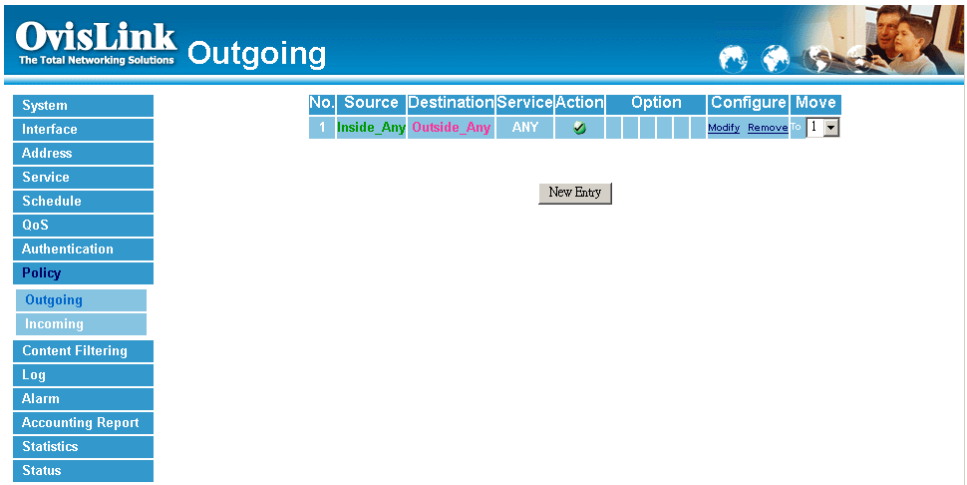
Step 6. Go to the **Outgoing** window under the **Policy** menu.

Step 7. Click the **New Entry** button.

Step 8. In **Add New Policy** window, set each parameter, then click **OK**.



Step 9. Open all the services (ANY). The setup is completed.



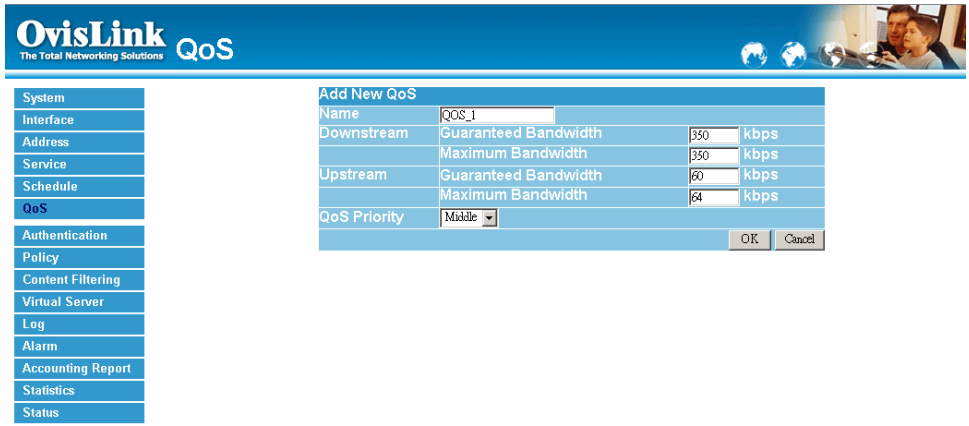
Install a server inside the LAN network, open to all the IP addresses including LAN and WAN IPs to use QoS to attain the maximum downstream and upstream bandwidth. The setup orders should be QoS, Virtual Server and then Policy.

Step 1. Enter the **QoS** window in the menu bar on the left hand side of the window.

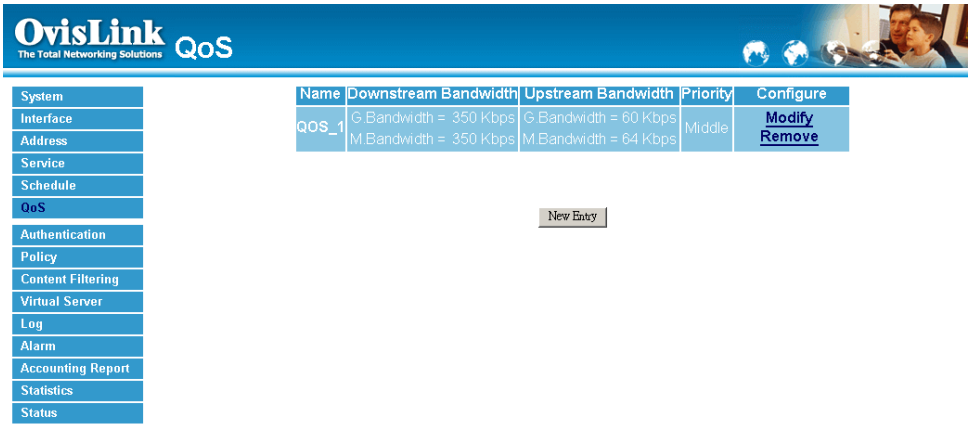
Step 2. Click the **New Entry** button.

Step 3. In the **Add New QoS** window, enter each parameter.

Step 4. Click **OK**.

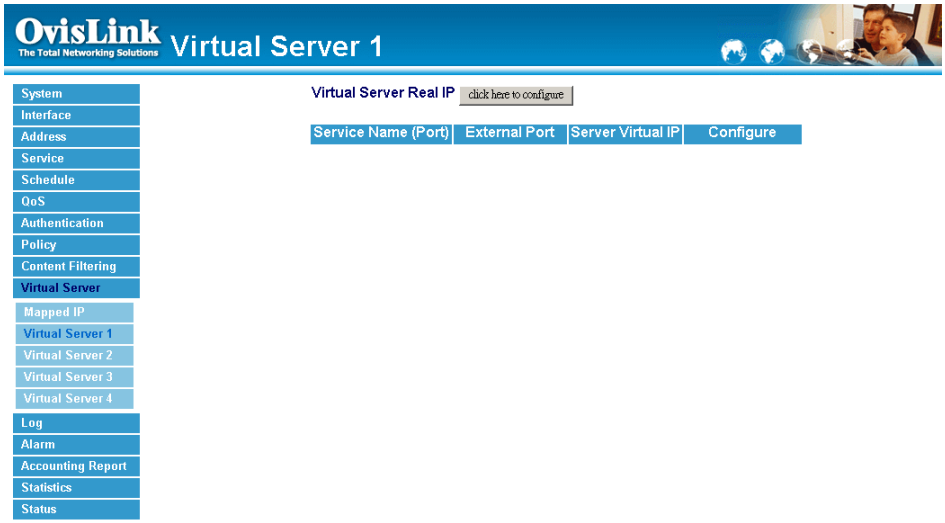


Step 5. When the following screen appears, the **QoS** setup is completed.

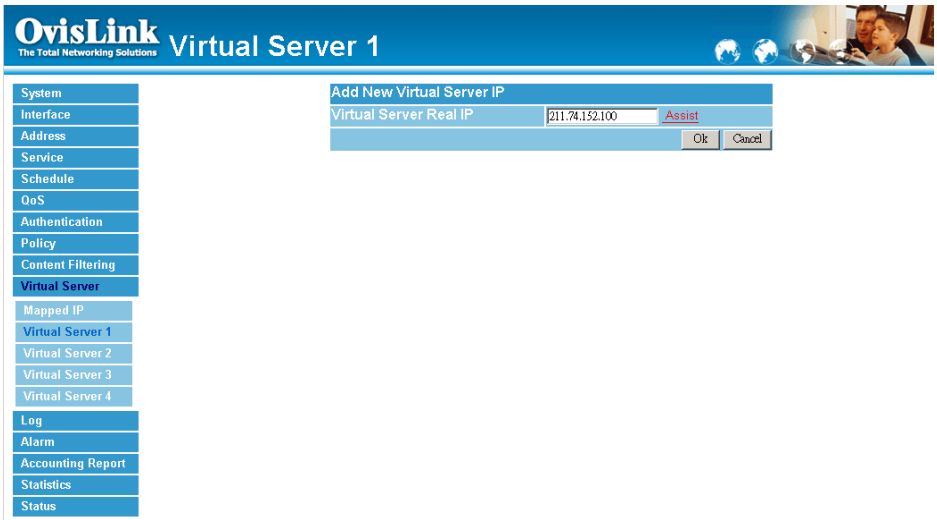


Step 6. Go to the **Virtual server 1** window under the **Virtual server** menu.

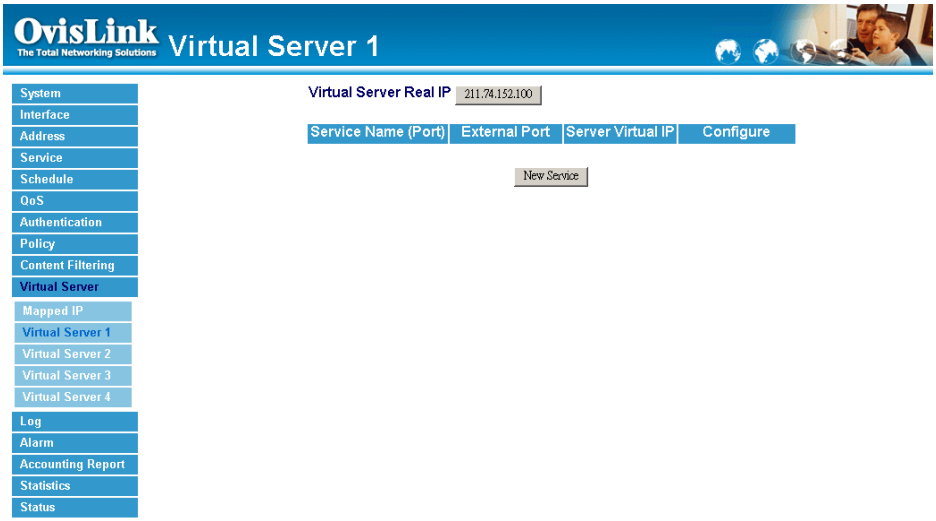
Step 7. Click the **Click here to configure** button.



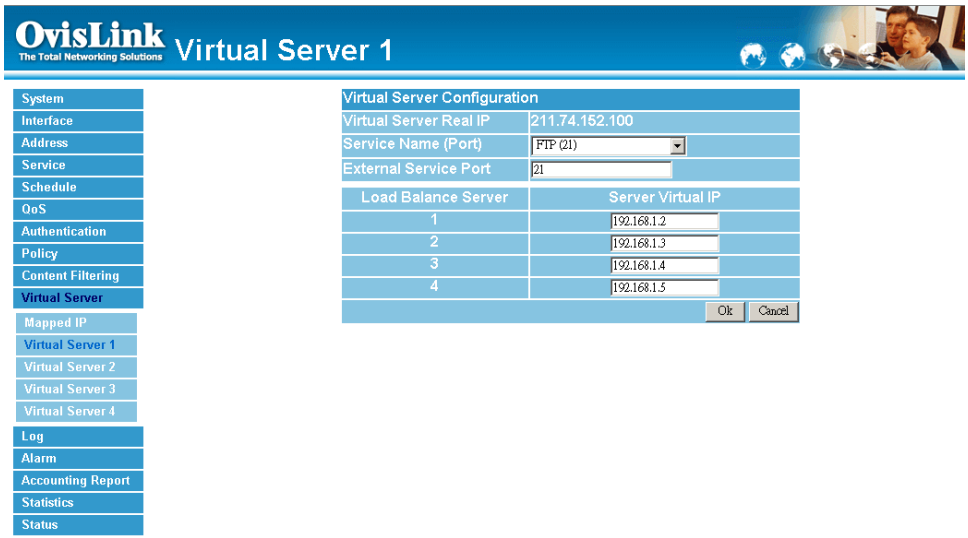
Step 8. In Virtual Server 1 window, enter the Virtual Server Real IP, and then click OK.



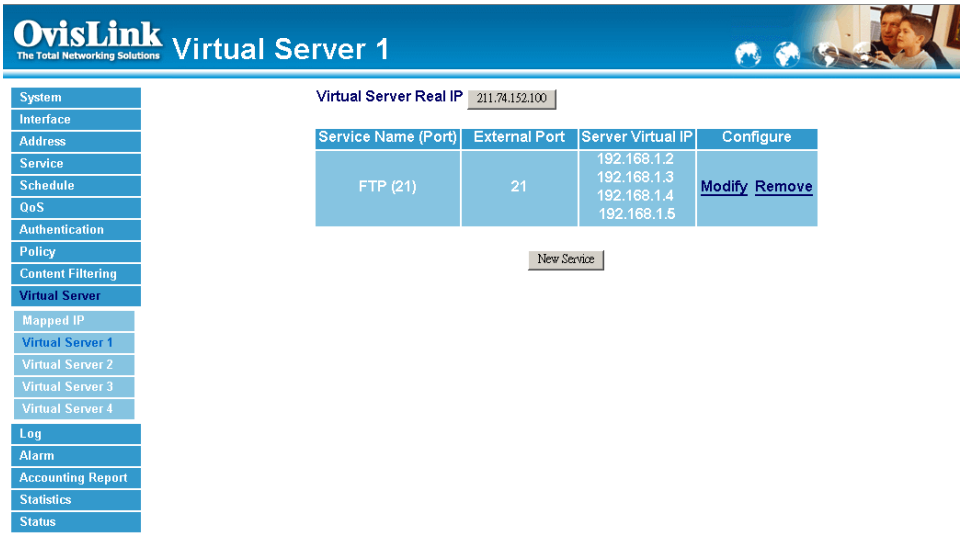
Step 9. After adding new server IP, click the **New Service** button.



Step 10. In the **Virtual Server Configuration** window, set each parameter, then click **OK**.

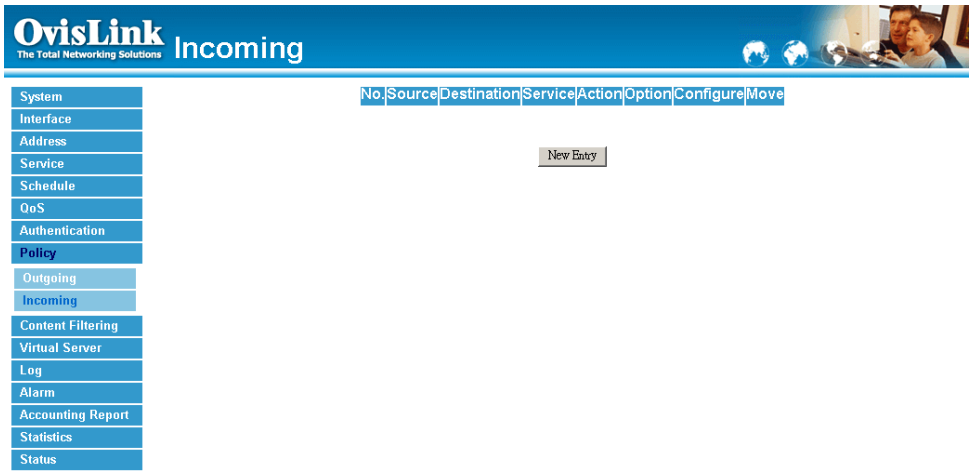


Step 11. When the following screen appears, the virtual server setup is complete.



Step 12. Enter the Incoming window under the Policy menu.

Step 13. Click the New Entry button.



Step 14. In the **Add New Policy** window, set each parameter, then click **OK.**